JUNIPER NETWORKS | Engineering Simplicity

Junos Space Network Management Platform

Complete Software Guide

Published
2020-11-09

Release
20.1

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Junos Space Network Management Platform Complete Software Guide
20.1
Copyright © 2020 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation | xlvii

Documentation and Release Notes | **xlvii**

Supported Platforms | **xlvii**

Documentation Conventions | **xlvii**

Documentation Feedback | **l**

Requesting Technical Support | **l**

- Self-Help Online Tools and Resources | **li**
- Creating a Service Request with JTAC | **li**

Guide 1 Getting Started Guide

1 **Junos Space Fabric Deployment**

Junos Space Fabric Architecture | 54

Junos Space Fabric Deployment Overview | 54

- Deploying a Junos Space Hardware Appliance | **55**
- Deploying a Junos Space Virtual Appliance | **56**
- Basic Requirements for a Fabric Deployment | **56**
- Configuring Network Connectivity for a Junos Space Fabric | **57**
- Adding Nodes to a Junos Space Fabric | **59**

2 **Junos Space System Administration**

Installing and Upgrading Junos Space Software Overview | 61

- Installing Junos Space Applications | **61**
- Upgrading Junos Space Applications | **62**
- Upgrading Junos Space Network Management Platform | **63**
- Uninstalling Junos Space Applications | **64**

Junos Space Applications Supported on the Junos Space Platform | 65

Junos Space License Installation Overview | 66

DMI Schema Overview | 67

Backing Up the Junos Space Platform Database | 68

Configuring User Access Controls Overview | 69

Authentication and Authorization Mode | **71**

Certificate–Based and Certificate Parameter–Based Authentication | **73**

User Roles | **73**

Remote Profiles | **74**

Domains | **75**

User Accounts | **75**

Device Partitions | **76**

3 **Junos Space Network Management**

Device Management in Junos Space Platform | 79

Discovering Devices | **80**

Authenticating Devices | **81**

Viewing the Device Inventory | **82**

Upgrading Device Images | **82**

Device Configuration Management in Junos Space Platform | 83

Modifying the Device Configuration by Using the Schema-Based Configuration Editor | **84**

Modifying the Device Configuration by Using Device Templates | **85**

Viewing Configuration Changes | **85**

Backing Up and Restoring Device Configuration Files | **86**

Guide 2 User Interface Guide

4 **Overview**

Junos Space User Interface Overview | 89

Junos Space Banner | **90**

Task Tree | **91**

Main Window | **93**

Junos Space Home Page Overview | 94

5

Working in the Junos Space User Interface

Logging In to Junos Space | 100

Setting and Accessing the Junos Space Home Page | 102

- Setting the Junos Space Home Page | **102**
- Accessing the Junos Space Home Page | **104**

Using the Getting Started Assistants on Junos Space | 104

Accessing Help on Junos Space | 106

Understanding GUI Controls | 106

- Check Box | **107**
  - Selecting All Objects on a Single Page | **107**
  - Selecting All Objects Across Multiple Pages | **108**
- Date Picker | **110**
- Drop-down List | **111**
- Option Button | **112**
- Search Field | **112**
- Spin Box | **113**
- Slider | **113**
- Text Box | **114**
  - Identifying the Range of Values | **115**
- Tree View | **116**
- Scrolling Controls | **117**
- Sizing Controls | **118**

Understanding Tooltips and Messages | 118

- Error Messages | **119**
- Confirmation Messages | **120**
- Information Messages | **120**
- Standard Icons in Messages | **121**

Understanding Status Indicators | 123

- Progress Bars | **124**
- Status Indicator Icons | **124**

Viewing the Junos Space Platform Dashboard | 126

Workspace Statistics Page Overview | 128

Workspace Statistics | **128**

Inventory Landing Page Overview | 129

Organizing Your View | **130**

Paging Controls | **131**

Sorted-by Indicator | **131**

Show or Hide Columns | **132**

Filter Submenus | **133**

Working with Objects on an Inventory Page | **134**

Toolbar Icons | **134**

Actions Menu and Shortcut Menu | **134**

Exporting Data | **135**

Filter Management in Junos Space Platform User Interface | 137

Understanding Filtering Options in Junos Space Platform User Interface | **137**

Overview | **138**

Benefits | **139**

Pages and Columns that Support Filtering | **139**

Managing Filtering Options | **150**

Creating Filters by Manually Entering the Filter Criteria | **150**

Creating Filters by Using the Filter Submenu Options | **153**

Saving a Filter | **155**

Modifying a Filter | **155**

Creating a Public Filter | **156**

Applying a Filter | **157**

Clearing a Filter | **157**

Deleting a Filter | **157**

Error Conditions and Error Messages for Filters | **158**

Global Search Overview | 164

Using Global Search | 173

Viewing Your Jobs | 175

Changing Your Password on Junos Space | 177

Logging Out of Junos Space | 178

Guide 3 Workspaces User Guide

1 **Overview**

Introduction | 182

Junos Space Platform Workspaces Overview | **182**

Viewing the Junos Space Platform Dashboard | **184**

2 **Devices**

Device Management | 189

Device Management Overview | **189**

- Managed and Unmanaged Devices | **190**
- IPv4 and IPv6 Address Support | **191**

Confirmed-commit from Junos Space Network Management Platform | **191**

Viewing Managed Devices | **194**

Juniper Networks Devices Supported by Junos Space Network Management Platform | **199**

Uploading Device Tags by Using a CSV File | **211**

Filtering Devices by CSV | **212**

Systems of Record | 214

Systems of Record in Junos Space Overview | **214**

- Systems of Record | **214**
- Implications on device management | **215**

Understanding How Junos Space Automatically Resynchronizes Managed Devices | **216**

- Network as System of Record | **216**
- Junos Space as System of Record | **218**

Device Discovery Profiles | 220

Device Discovery Profiles Overview | **220**

- Connections Initiated by Junos Space or the Device | **221**
- Device Information Fetched During Device Discovery | **225**

Creating a Device Discovery Profile | **226**

- Specifying Device Targets | **227**
- Specifying Probes | **230**
- Selecting the Authentication Method and Specifying Credentials | **233**
- (Optional) Specifying SSH Fingerprints | **235**
- Scheduling Device Discovery | **235**

Running Device Discovery Profiles | **238**

Modifying a Device Discovery Profile | **239**

Cloning a Device Discovery Profile | **241**

Viewing a Device Discovery Profile | **243**

Deleting Device Discovery Profiles | **244**

Exporting the Device Discovery Details As a CSV File | **245**

Modeling Devices | 246

Rapid Deployment Overview | **247**

Zero Touch Deployment Using Autoinstallation and Junos Space Network Management Platform on ACX Series and SRX Series Devices | **248**

- Zero-Touch Deployment Using the Autoinstallation and Model and Activate Devices Features | **250**
- Zero-Touch Deployment Using the Autoinstallation Feature and the Configuration Server | **250**

Model Devices Overview | **251**

Creating a Connection Profile | **252**

Creating a Modeled Instance | **257**

Activating a Modeled or Cloned Device in Junos Space Network Management Platform | **262**

Downloading a Configlet | **266**

Viewing and Copying Configlet Data | **268**

Activating Devices by Using Configlets | **269**

- Activating a Device by Using a Plain-text Single Configlet | **270**
- Activating a Device by Using an AES-encrypted Single Configlet | **270**
- Activating a Device by Using a Plain-text Bulk Configlet | **271**
- Activating a Device by Using an AES-encrypted Bulk Configlet | **271**

Viewing a Modeled Instance | 272

Adding More Devices to an Existing Modeled Instance | 274

Viewing the Status of Modeled Devices | 275

Deleting Modeled Instances | 276

Viewing a Connection Profile | 276

Cloning a Connection Profile | 278

Modifying a Connection Profile | 278

Deleting Connection Profiles | 279

Device Authentication in Junos Space | 281

Device Authentication in Junos Space Overview | 281

- Credentials-Based Device Authentication | 282
- Key-Based Device Authentication | 282
- SSH Fingerprint-Based Device Authentication | 283
- Supported Algorithms for Junos Space SSH | 284

Generating and Uploading Authentication Keys to Devices | 285

- Generating Authentication Keys | 286
- Uploading Authentication Keys to Multiple Managed Devices for the First Time | 287
- Uploading Authentication Keys to Managed Devices With a Key Conflict | 290

Resolving Key Conflicts | 291

Modifying the Authentication Mode on the Devices | 293

Acknowledging SSH Fingerprints from Devices | 295

Viewing Device Inventory | 299

Device Inventory Overview | 299

- Inventory for Aggregation and Satellite Devices | 300

Viewing the Physical Inventory | 301

Displaying Service Contract and EOL Data in the Physical Inventory Table | 305

Viewing Physical Interfaces of Devices | 306

Viewing Logical Interfaces | 308

Viewing and Acknowledging Inventory Changes on Devices | 309

Exporting Device Inventory | 312

Exporting the License Inventory | 312

Viewing and Exporting the Software Inventory of Managed Devices | 316

Exporting the Physical Inventory of Devices | 318

Configuring Juniper Networks Devices | 321

Modifying the Configuration on the Device | 322

Reviewing and Deploying the Device Configuration | 327

- Viewing the Configuration Changes on the Device | 328
- Validating the Delta Configuration on the Device | 330
- Viewing the Device-Configuration Validation Report | 330
- Excluding or Including a Group of Configuration Changes | 331
- Deleting a Group of Configuration Changes | 331
- Approving the Configuration Changes | 332
- Rejecting the Configuration Changes | 333
- Deploying the Configuration Changes to a Device | 333

Junos OS Releases Supported in Junos Space Network Management Platform | 334

Configuration Guides Overview | 337

Saving the Configuration Created using the Configuration Guides | 337

Previewing the Configuration Created using the Configuration Guides | 338

Deploying the Configuration Created using the Configuration Guides | 339

Viewing and Assigning Shared Objects | 340

Applying a CLI Configlet to Devices | 342

Applying a CLI Configlet to a Physical Inventory Element | 346

Applying a CLI Configlet to a Physical Interface | 350

Applying a CLI Configlet to a Logical Interface | 354

Executing a Script on the Devices | 358

Executing a Script on a Physical Inventory Component | 363

Executing a Script on a Logical Interface | 365

Executing a Script on the Physical Interfaces | 367

Device Adapter | 371

Worldwide Junos OS Adapter Overview | 371

Installing the Worldwide Junos OS Adapter | 372

Connecting to ww Junos OS Devices | 374

Device Configuration Management | 376

Viewing the Active Configuration | **376**

Viewing the Configuration Change Log | **381**

Resolving Out of band Changes | **382**

Creating a Quick Template from the Device Configuration | **384**

Adding and Managing Non Juniper Networks Devices | 386

Adding Unmanaged Devices | **386**

Modifying Unmanaged Device Configuration | **389**

Accessing Devices | 391

Launching a Device's Web User Interface | **391**

Looking Glass Overview | **392**

Executing Commands by Using Looking Glass | **393**

Exporting Looking Glass Results in Junos Space Network Management Platform | **395**

Secure Console Overview | **396**

Connecting to a Device by Using Secure Console | **397**

- Connecting to a Managed Device from the Device Management Page | **398**
- Connecting to an Unmanaged Device from the Device Management Page | **401**
- Connecting to a Managed or Unmanaged Device from the Secure Console Page | **403**

Configuring SRX Device Clusters in Junos Space using Secure Console | **405**

- Configuring a Standalone Device from a Single-node Cluster | **405**
- Configuring a Standalone Device from a Two-Node Cluster | **408**
- Configuring a Primary Peer in a Cluster from a Standalone Device | **410**
- Configuring a Secondary Peer in a Cluster from a Standalone Device | **413**
- Configuring a Cluster with Loopback Interface | **415**

Logical Systems (LSYS) | 417

Understanding Logical Systems for SRX Series Services Gateways | **417**

Creating a Logical System (LSYS) | **418**

Deleting Logical Systems | **419**

Viewing Logical Systems for a Physical Device | **420**

Viewing the Physical Device for a Logical System | **420**

Device Partitions | 422

Creating Device Partitions | **422**

Modifying Device Partitions | **423**

Deleting Device Partitions | **424**

Custom Labels | 426

Adding Custom Labels | **426**

- Adding Custom Labels for a Device | **427**
- Adding Custom Labels for Physical Inventory | **428**
- Adding Custom Labels for a Physical Interface | **429**
- Adding Custom Labels for a Logical Interface | **429**

Importing Custom Labels | **430**

Modifying Custom Labels | **432**

Deleting Custom Labels | **433**

Verifying Template, Image Deployment, Script Execution, and Staged Images on Devices | 434

Viewing the Device-Template Association (Devices) | **434**

Viewing Associated Scripts | **437**

Viewing Script Execution | **437**

Viewing Staged Images on a Device | **438**

Device Monitoring | 441

Viewing Alarms from a Managed Device | **441**

Viewing the Performance Graphs of a Managed Device | **443**

Device Maintenance | 446

Viewing Device Statistics | **446**

Viewing Devices and Logical Systems with QuickView | **447**

Resynchronizing Managed Devices with the Network | **448**

Putting a Device in RMA State and Reactivating Its Replacement | **449**

- Putting a Device in RMA State | **450**
- Reactivating a Replacement Device | **451**

Modifying the Target IP Address of a Device | **453**

Modifying the Serial Number of a Device | **455**

Rebooting Devices | **456**

Deleting Staged Images on a Device | **457**

Cloning a Device in Junos Space Network Management Platform | **458**

Deleting Devices | **459**

3 **Device Templates**

Overview | 462

Device Templates Overview | **462**

- Template Definition | **464**
- Device Template States | **467**
- Device Template Statuses | **467**
- Device Templates Workflow | **467**
- Device Template Deployment | **469**

Template Definitions | 471

Creating a Template Definition | **471**

Finding Configuration Options in a Template Definition | **478**

Working with Rules in a Template Definition | **480**

Specifying Device-Specific Values in Template Definitions | **482**

- Creating a CSV file with device-specific values | **482**
- Using a CSV file to set device-specific values | **483**

Managing CSV Files for a Template Definition | **485**

Publishing a Template Definition | **486**

Viewing a Template Definition | **486**

Modifying a Template Definition | **488**

Cloning a Template Definition | **489**

Importing a Template Definition | **490**

Exporting a Template Definition | **491**

Unpublishing a Template Definition | **492**

Deleting a Template Definition | **493**

Configuring Devices using Device Templates | 494

Creating a Device Template | **494**

Assigning a Device Template to Devices | **496**

Deploying a Template to the Devices | 498

Modifying a Device Template | 502

Undeploying a Device Template from the Devices | 503

Unassigning a Device Template from the Devices | 504

Auditing a Device Template Configuration | 505

Configuring Devices using Quick Templates | 508

Quick Templates Overview | 508

Creating a Quick Template | 509

Deploying a Quick Template | 515

Device Template Administration | 520

Viewing Template Details | 520

Viewing the Device-Template Association (Device Templates) | 521

Viewing Template Definition Statistics | 524

Viewing Device Template Statistics | 525

Comparing Templates or Template Versions | 525

Comparing a Device Template Configuration with a Device Configuration | 527

Cloning a Template in Junos Space Network Management Platform | 529

Exporting and Importing a Quick Template in Junos Space Network Management Platform | 530

- Exporting a Quick Template | 530
- Importing a Quick Template | 531

Deleting Device Templates from Junos Space Network Management Platform | 532

4 **CLI Configlets**

Overview | 534

CLI Configlets Overview | 534

- Configlet Variables | 535
  - Default Variables | 535
  - User-Defined Variables | 536
  - Predefined Variables | 536
- Velocity Templates | 536
- Directives | 536

CLI Configlets Workflow | 537

Configlet Context | **541**

- Context of an Element | **542**
- Context filtering | **544**

Nesting Parameters | **546**

CLI Configlets | 548

Creating a CLI Configlet | **548**

Modifying a CLI Configlet | **552**

Viewing CLI Configlet Statistics | **552**

Viewing a CLI Configlet | **553**

Exporting CLI Configlets | **556**

CLI Configlet Examples | **557**

- Example 1: Setting the description of a physical interface | **557**
- Example 2: Setting the vlan of a logical interface, where the vlan id is chosen from a predefined set of values | **558**
- Example 3: Setting a description on all the interfaces of a device | **559**
- Example 4: Setting a configuration in all the PICs belonging to a device and certain configuration only on the first PIC of FPC 0 | **561**
- Example 5: Halting the description of a physical interface | **564**
- Example 6: Deleting configuration from a physical interface | **565**

Deleting CLI configlets | **565**

Cloning a CLI Configlet | **566**

Importing CLI Configlets | **567**

Applying a CLI Configlet to Devices | **573**

Comparing CLI Configet Versions | **577**

Marking and Unmarking CLI Configlets as Favorite | **578**

- Marking CLI Configlets as Favorite | **579**
- Unmarking CLI Configlets Marked as Favorite | **579**

Configuration Views | 581

Configuration Views Overview | **581**

Configuration View Variables | **582**

Configuration View Workflow | **583**

XML Extensions | **585**

Creating a Configuration View | **586**

Viewing a Configuration View | **588**

Modifying a Configuration View | **589**

Deleting Configuration Views | **590**

Exporting and Importing Configuration Views | **591**

- Exporting Configuration Views | **592**
- Importing Configuration Views | **593**

Viewing Configuration Views Statistics | **595**

Default Configuration Views Examples | **595**

- Default view | **596**
- Example XML view | **596**
- Example Form view | **597**
- Example Grid view | **598**

XPath and Regular Expressions | 600

XPath and Regex Overview | **600**

Creating Xpath or Regex | **601**

Modifying Xpath and Regex | **601**

Deleting Xpath and Regex | **602**

XPath and Regular Expression Examples | **603**

- Example 1 – Alphanumeric | **603**
- Example 2 - Logical Interfaces per Physical Interface | **603**
- Example 3 – Physical Interfaces | **603**
- Example 4 – Devices | **604**

Configuration Filters | 605

Creating a Configuration Filter | **605**

Modifying a Configuration Filter | **606**

Deleting Configuration Filters | **607**

5

Images and Scripts

Overview | 609

Device Images and Scripts Overview | **609**

Viewing Statistics for Device Images and Scripts | **610**

Managing Device Images | 613

Device Images Overview | **613**

Importing Device Images to Junos Space | **615**

Viewing Device Images | **616**

Modifying Device Image Details | **618**

Staging Device Images | **620**

Staging Satellite Software Packages on Aggregation Devices | **625**

Verifying the Checksum | **630**

Viewing and Deleting MD5 Validation Results | **634**

- Viewing the MD5 Validation Results | **635**
- Deleting the MD5 Validation Results | **636**

Deploying Device Images | **637**

Deploying Satellite Software Packages on Aggregation and Satellite Devices | **652**

Viewing Device Image Deployment Results | **657**

Viewing Device Association of Images | **659**

Undeploying JAM Packages from Devices | **661**

Removing Device Images from Devices | **666**

Deleting Device Images | **671**

Managing Scripts | 672

Scripts Overview | **673**

Promoting Scripts Overview | **676**

Importing Scripts to Junos Space | **676**

- Importing Scripts from Files | **677**
- Importing Scripts from a Git Repository | **678**

Viewing Script Details | **681**

Modifying Scripts | **684**

Modifying Script Types | **687**

Comparing Script Versions | **688**

Staging Scripts on Devices | **689**

Verifying the Checksum of Scripts on Devices | **693**

Viewing Verification Results | **695**

Enabling Scripts on Devices | **696**

Executing Scripts on Devices | **700**

Executing Scripts on Devices Locally with JUISE | **704**

Viewing Execution Results | **708**

Exporting Scripts in .tar Format | **709**

Viewing Device Association of Scripts | **710**

Marking and Unmarking Scripts as Favorite | **711**

- Marking Scripts as Favorite | **712**
- Unmarking Scripts Marked as Favorite | **712**

Disabling Scripts on Devices | **713**

Removing Scripts from Devices | **716**

Deleting Scripts | **720**

Script Annotations | **721**

- Script Execution Types | **724**
- Variable Context | **725**
- Local Script Execution | **726**
- Nesting Variables | **727**

Script Example | **727**

Managing Operations | 730

Operations Overview | **730**

Creating an Operation | **731**

Importing an Operation | **736**

Viewing an Operation | **738**

Modifying an Operation | **740**

Running an Operation | **740**

Viewing Operation Results | **744**

Copying an Operation | **745**

Exporting an Operation in .tar Format | **746**

Deleting an Operation | **748**

Managing Script Bundles | 749

Script Bundles Overview | **749**

Creating a Script Bundle | **750**

Viewing Script Bundles | **753**

Modifying a Script Bundle | **754**

Staging Script Bundles on Devices | **755**

Enabling Scripts in Script Bundles on Devices | **758**

Executing Script Bundles on Devices | **760**

Disabling Scripts in Script Bundles on Devices | **763**

Viewing Device Associations of Scripts in Script Bundles | **765**

Deleting Script Bundles | **765**

6 **Reports**

Reports Overview | 768

Reports Overview | **768**

- Audit Trail Report Type | **770**
- Device Inventory Report Type | **770**
- Device License Inventory Report Type | **771**
- Device Logical Interface Inventory Report Type | **772**
- Device Physical Interface Inventory Report Type | **774**
- Device Physical Inventory Report Type | **775**
- Device Software Inventory Report Type | **776**
- Job Inventory Report Type | **777**
- User Account Report Type | **778**

Report Definitions | 780

Creating Report Definitions | **780**

Viewing Report Definitions | **783**

Modifying Report Definitions | **784**

Cloning Report Definitions | **785**

Deleting Report Definitions | **786**

Viewing Report Definition Statistics | **787**

Reports | 788

Generating Reports | **789**

Viewing a Report | **792**

Viewing and Downloading Generated Reports | **794**

Deleting Generated Reports | **795**

Viewing Report Statistics | **795**

7 **Network Monitoring**

Overview | 798

Network Monitoring Workspace Overview | **799**

Working with the Network Monitoring Home Page | **802**

- Viewing Nodes with Pending Problems | **802**
- Viewing Nodes with Outages | **803**
- Availability Over the Past 24 Hours | **803**
- Viewing Outstanding Notifications | **804**
- Viewing Resource Graphs | **804**
- Viewing KSC Reports | **805**
- Searching for Nodes by Using Quick Search | **806**

Managing Nodes | 809

Viewing the Node List | **809**

Managing Surveillance Categories | **811**

- Modifying Surveillance Categories | **811**
- Deleting Surveillance Categories | **811**
- Adding Surveillance Categories | **812**

Resynchronizing Nodes in Network Monitoring | **813**

Turning SNMP Data Collection Off and On | **814**

Searching for Nodes and Assets | 816

Searching for Nodes or Nodes with Asset Information | **816**

- Searching for Nodes | **816**
- Searching for Nodes with Asset Information | **818**

Working with Node Assets | **820**

- Searching for and Viewing Nodes with Asset Information | **820**
- Viewing and Modifying Node Asset Information | **821**

Managing Outages | 823

Viewing and Tracking Outages | **823**

- Viewing Details about an Outage | **824**
- Viewing the List of Outages | **825**

Configuring Scheduled Outages | **826**

Using the Network Monitoring Dashboard | 828

Viewing the Network Monitoring Dashboard | **828**

- Using the Dashboard Surveillance View | **829**

Managing and Configuring Events | 833

Viewing and Managing Events | **833**

- Viewing the Details of an Event | **834**
- Searching for Events (Advanced Event Search) | **835**
- Viewing, Searching for, Sorting, and Filtering Events | **837**

Selecting and Sending an Event to the Network Management System | **840**

Managing Events Configuration Files | **841**

- Adding New Events Configuration Files | **841**
- Deleting Events Configuration Files | **842**
- Modifying Events Configuration Files | **842**

Managing and Configuring Alarms | 844

Viewing and Managing Alarms | **844**

- Viewing Details of an Alarm and Acting on an Alarm | **846**
- Viewing Alarms in Summary and Detailed Views | **849**
- Viewing NCS Alarms | **855**

Searching for Alarms (Advanced Alarms Search) | **856**

Alarm Notification Configuration Overview | **857**

Basic Filtering | **857**

Guidelines for Configuring Alarm Notifications | **858**

Advanced Filtering | **859**

Configuring Alarm Notification | **860**

Configuring a Basic Filter for Alarm Notification | **861**

Activating Alarm Notification Configuration Files for Basic Filtering | **863**

Reloading a Filter Configuration to Apply Filter Configuration Changes | **863**

Managing and Configuring Notifications | 865

Viewing, Configuring, and Searching for Notifications | **865**

Notification Escalation | **866**

Configuring Event Notifications, Path Outages, and Destination Paths | **867**

Configuring Event Notifications | **867**

Configure Destination Paths | **869**

Configure Path Outages | **871**

Managing Reports and Charts | 873

Network Monitoring Reports Overview | **873**

Resource Graphs | **873**

Key SNMP Customized Performance Reports, Node Reports, and Domain Reports | **874**

Database Reports | **874**

Statistics Reports | **874**

Creating Reports | **874**

Creating Key SNMP Customized Performance Reports, Node Reports, and Domain Reports | **875**

Creating a New KSC Report from an Existing Report | **875**

Viewing Reports | **876**

Viewing Resource Graphs | **877**

Viewing Key SNMP Customized (KSC) Performance Reports, Node Reports, and Domain Reports | **877**

Viewing Database Reports | **878**

Sending Database Reports | **878**

Viewing Pre-run Database Reports | **880**

Viewing Statistics Reports | **880**

Generating a Statistics Report for Export | 880

Deleting Reports | 881

Deleting Key SNMP Customized Reports | 882

Deleting Pre-Run Database Reports | 882

Viewing Charts | 883

Network Monitoring Topology | 884

Network Monitoring Topology Overview | 885

Working with Topology | 887

Using the Search Option to View Nodes | 888

Working with Topology Views | 889

Viewing the Events and Alarms Associated with a Node | 890

Viewing Alarms and Node Details | 891

Viewing Nodes with Active Alarms | 893

Managing Alarms Associated with Nodes | 893

Viewing the Topology with Different Layouts | 893

Automatic Refresh of the Topology | 894

Viewing the Status of Node Links | 895

Viewing the Alarm State of Services Links | 895

Pinging a Node | 895

Viewing the Resource Graphs Associated with the Node | 896

Connecting to a Device by Using SSH | 897

Network Monitoring Topology Discovery Methods Supported by Junos Space Network Management Platform | 899

Network Monitoring Administration | 901

Configuring Network Monitoring System Settings | 901

Network Monitoring System Information | 902

Generating a Log File for Troubleshooting | 903

Changing the Notification Status | 903

Updating Network Monitoring After Upgrading the Junos Space Network Management Platform | 904

Overview | 904

Step 1: Monitoring the Software Install Status Window for File Conflicts | 904

Step 2: Identifying Files with Conflicts | 906

Step 3: Merging Files with Conflicts | **908**

Step 4: Verifying the Manual Merge Status of Configuration Files | **909**

Step 5: Final Steps After Upgrading Network Monitoring | **910**

Configuring SNMP Community Names by IP | **912**

Configuring SNMP Data Collection per Interface | **913**

Managing Thresholds | **913**

Creating Thresholds | **914**

Modifying Thresholds | **916**

Deleting Thresholds | **917**

Compiling SNMP MIBs | **918**

Uploading MIBs | **918**

Compiling MIBs | **919**

Viewing MIBs | **919**

Deleting MIBs | **920**

Clearing MIB Console Logs | **920**

Generating Event Configuration | **920**

Generating a Data Collection Configuration | **922**

Managing SNMP Collections | **924**

Adding a New SNMP Collection | **924**

Modifying an SNMP Collection | **925**

Managing SNMPv3 Trap Configuration | **926**

Managing Data Collection Groups | **929**

Adding New Data Collection Files | **930**

Deleting Data Collection Files | **930**

Modifying Data Collection Files | **931**

Managing and Unmanaging Interfaces and Services | **933**

Starting, Stopping, and Restarting Services | **933**

8 Configuration Files

Overview | 938

Managing Configuration Files Overview | 938

Viewing Configuration File Statistics | 940

Managing Configuration Files | 942

Backing Up Configuration Files | 943

Viewing Configuration Files | 948

Comparing Configuration Files | 953

Modifying Configuration Files | 955

Restoring Configuration Files | 958

Exporting Configuration Files | 960

Deleting Configuration Files | 962

9 Jobs

Overview | 965

Jobs Overview | 965

Managing Jobs | 968

Viewing Statistics for Jobs | 968

- Viewing the Types of Jobs That Are Run | 969
- Viewing the State of Jobs That Have Run | 969
- Viewing Average Execution Times for Jobs | 970

Viewing Your Jobs | 970

Viewing Jobs | 972

Viewing Objects on Which a Job is Executed | 975

Viewing Job Recurrence | 978

Rescheduling and Modifying the Recurrence Settings of Jobs | 978

Retrying a Job on Failed Devices | 980

Reassigning Jobs | 982

Canceling Jobs | 985

Clearing Your Jobs | **986**

Archiving and Purging Jobs | **987**

- Purging Jobs Without Archiving | **987**
- Archiving Jobs to a Local Server and Purging the Jobs from the Database | **989**
- Archiving Jobs to a Remote Server and Purging the Jobs from the Database | **990**

Common Error Messages in Device-Related Operations | **992**

10 **Role-Based Access Control**

Overview | 995

Role-Based Access Control Overview | **995**

- User Authentication | **995**
- RBAC Enforcement | **996**
  - RBAC Enforcement by Workspace | **996**
  - RBAC Enforcement Not Supported on the Getting Started Page | **996**

Roles | 997

Roles Overview | **998**

Predefined Roles Overview | **999**

Creating a User-Defined Role | **1022**

Managing Roles | **1024**

- Viewing User Role Details | **1024**
- Managing Predefined and User-Defined Roles | **1025**

Modifying User-Defined Roles | **1026**

Deleting User-Defined Roles | **1027**

Cloning Predefined and User-Defined Roles | **1028**

Exporting User-Defined Roles from Junos Space Network Management Platform | **1030**

Importing Roles to Junos Space Network Management Platform | **1031**

User Accounts | 1033

Configuring Users to Manage Objects in Junos Space Overview | **1033**

- User-Specific Idle Timeout | **1034**

Creating Users in Junos Space Network Management Platform | **1035**

- Creating a User | **1036**

Modifying a User | **1044**

Deleting Users | **1050**

Disabling and Enabling Users | **1051**

Unlocking Users | **1053**

Viewing Users | **1054**

- Sorting Columns | **1055**
- Displaying or Hiding Columns | **1055**
- Filtering Users | **1056**
- Viewing User Details | **1057**
- Performing Actions on Users | **1060**

Exporting User Accounts from Junos Space Network Management Platform | **1061**

- Creating a User Accounts Report Definition | **1062**
- Generating and Downloading a Report | **1063**

Changing Your Password on Junos Space | **1065**

Clearing User Local Passwords | **1067**

Viewing User Statistics | **1068**

- Viewing the Number of Users Assigned by Role | **1068**

User Groups | 1069

User Groups Overview | **1069**

Managing User Groups | **1070**

- Creating a User Group | **1070**
- Modifying a User Group | **1072**
- Deleting a User Group | **1073**

Job Management Using User Groups | **1074**

- Job Visibility for User Assigned to User Group(s) | **1074**

Domains | 1077

Domains Overview | **1077**

- Accessing Objects In and Across Domains | **1078**
- Device Partitions | **1080**
- Assignment of Objects to Domains | **1083**

Working with Domains | **1085**

- Adding a Domain | **1085**
- Modifying a Domain | **1087**
- Deleting Domains | **1089**

Switching from One Domain to Another | **1092**

Assigning Objects to an Existing Domain | **1092**

Assigning Users to an Existing Domain from the Domains Page | **1093**

Assigning Devices to an Existing Domain from the Domains Page | **1094**

Assigning Remote Profiles to an Existing Domain from the Domains Page | **1095**

Assigning Objects to an Existing Domain from the Inventory Landing Pages | **1095**

Exporting Domains from Junos Space Network Management Platform | **1096**

Remote Profiles | 1098

Creating a Remote Profile | **1098**

Modifying a Remote Profile | **1100**

Deleting Remote Profiles | **1101**

API Access Profiles | 1102

Creating an API Access Profile | **1102**

Modifying an API Access Profile | **1104**

Deleting API Access Profiles | **1105**

User Sessions | 1106

User Sessions Overview | **1106**

Limiting User Sessions in Junos Space | **1108**

Terminating User Sessions | **1110**

Using the Junos Space CLI to View Users Logged In to the Junos Space GUI | **1111**

11 **Audit Logs**

Overview | 1115

Junos Space Audit Logs Overview | **1115**

Managing Audit Logs | 1117

Viewing Audit Logs | **1117**

Viewing Audit Log Statistics | **1121**

Viewing the Dynamic Audit Log Statistical Graph | **1121**

Viewing the Top 10 Active Users In 24 Hours Statistics | **1123**

Exporting Audit Logs | **1123**

Converting the Junos Space Audit Log File Timestamp from UTC to Local Time Using Microsoft Excel | **1125**

Archiving and Purging or Only Purging Audit Logs | **1126**

- Purging Audit Logs Without Archiving | **1127**
- Purging Audit Logs After Archiving | **1130**

12 **Administration**

Overview | 1136

Junos Space Administrators Overview | **1136**

Viewing the Administration Statistics | **1138**

- Viewing System Health Information | **1139**
- Viewing the System Health Report | **1139**
- Viewing System Alert Messages in the Last 30 Days | **1150**

Junos Space IPv6 Support Overview | **1152**

Maintenance Mode Overview | **1153**

- Maintenance Mode Access and System Locking | **1154**
- Maintenance-Mode User Administration | **1155**

Managing Nodes in the Junos Space Fabric | 1156

Fabric Management Overview | **1157**

Overall System Condition and Fabric Load History Overview | **1159**

- Overall System Condition | **1159**
- Fabric Load History | **1160**
- Active Users History | **1161**

Junos Space Nodes and FMPM Nodes in the Junos Space Fabric Overview | **1162**

- Understanding the Junos Space Node Functions in a Fabric | **1162**
- Understanding the FMPM Node Functions in a Fabric | **1166**

Dedicated Database Nodes in the Junos Space Fabric Overview | **1169**

Cassandra Nodes in the Junos Space Fabric Overview | **1172**

Adding a Node to an Existing Junos Space Fabric | **1176**

- Adding a Junos Space Node to the Junos Space Fabric | **1177**
- Adding an FMPM Node to the Junos Space Fabric | **1182**
- Obtaining Fingerprint of a Junos Space Node | **1183**

Starting the Cassandra Service on a Junos Space Node | **1185**

Viewing Nodes in the Fabric | **1186**

- Changing Views | **1186**
- Viewing Fabric Node Details | **1187**

Monitoring Nodes in the Fabric | **1194**

- Viewing and Modifying the SNMP Configuration for a Fabric Node | **1194**
- Starting SNMP Monitoring on Fabric Nodes | **1248**
- Stopping SNMP Monitoring on Fabric Nodes | **1249**
- Restarting SNMP Monitoring on Fabric Nodes | **1250**
- Adding a Third-Party SNMP V1 or V2c Manager on a Fabric Node | **1250**
- Adding a Third-Party SNMP V3 Manager on a Fabric Node | **1251**
- Deleting a Third-Party SNMP Manager from a Fabric Node | **1253**
- Installing StorMan RPM for Monitor RAID Functionality | **1253**

Viewing Alarms from a Fabric Node | **1254**

Shutting Down or Rebooting Nodes in the Junos Space Fabric | **1256**

Disabling the Cassandra Service on a Junos Space Node | **1258**

Deleting a Node from the Junos Space Fabric | **1259**

Resetting MySQL Replication | **1262**

Modifying the Network Settings of a Node in the Junos Space Fabric | **1264**

- Modifying the Fabric Virtual IP Address | **1266**
- Modifying the Network Settings of a Node | **1267**

Load-Balancing Devices Across Junos Space Nodes | **1271**

Replacing a Failed Junos Space Node | **1272**

Generating and Uploading Authentication Keys to Devices | **1272**

- Generating Authentication Keys | **1273**
- Uploading Authentication Keys to Multiple Managed Devices for the First Time | **1274**
- Uploading Authentication Keys to Managed Devices With a Key Conflict | **1277**

Configuring the ESX or ESXi Server Parameters on a Node in the Junos Space Fabric | **1278**

Creating a System Snapshot | **1279**

Deleting a System Snapshot | **1281**

Restoring the System to a Snapshot | **1282**

Creating a Unicast Junos Space Cluster | **1284**

- Creating a Unicast Junos Space Cluster from a Single Node | **1285**
- Creating a Unicast Junos Space Cluster from an Existing Multicast Junos Space Cluster | **1286**
- Changing Unicast Communication to Multicast Communication on a Junos Space Cluster | **1287**

NAT Configuration for Junos Space Network Management Platform Overview | **1288**

- Using eth0 for Device Management Without a Dedicated Network Monitoring Node | **1290**
- Using eth3 for Device Management Without a Dedicated Network Monitoring Node | **1293**
- Using eth0 or eth3 for Device Management With a Dedicated Network Monitoring Node | **1296**

Configuring the NAT IP Addresses and Ports on Junos Space Platform | **1300**

Modifying the NAT IP Addresses and Ports on Junos Space Platform | **1302**

Disabling the NAT Configuration on Junos Space Platform | **1303**

Backing up and Restoring the Junos Space Platform Database | 1304

Backing Up and Restoring the Database Overview | **1305**

- Backing Up a Database | **1307**
- Restoring a Database | **1308**

Backing Up the Junos Space Network Management Platform Database | **1308**

Restoring the Junos Space Network Management Platform Database | **1314**

- Restoring the Junos Space Platform Database from a Local Backup File | **1315**
- Restoring the Junos Space Platform Database from a Remote Backup File | **1316**

Deleting Junos Space Network Management Platform Database Backup Files | **1319**

Viewing Database Backup Files | **1320**

- Changing Views | **1321**
- Viewing Database Details | **1321**
- Managing Database Commands | **1322**

Managing Licenses | 1323

Generating and Uploading the Junos Space License Key File | **1323**

- Generating the Junos Space License Key File | **1325**
- Uploading the Junos Space License Key File Contents | **1325**

Viewing Junos Space Licenses | **1326**

Managing Junos Space Platform and Applications | 1328

Managing Junos Space Applications Overview | **1328**

Upgrading Junos Space Network Management Platform Overview | **1330**

- Before You Begin | **1330**
- Pre-Upgrade Checks | **1331**
- How an Upgrade Impacts Previously Installed Junos Space Applications | **1331**
- Performing the Upgrade | **1332**

Junos Space Store Overview | **1333**

- About the Junos Space Store | **1333**
- Benefits of Junos Space Store | **1333**

Configuring and Managing Junos Space Store | **1334**

- Configuring Junos Space Store in Junos Space Network Management Platform | **1334**
- Modifying Junos Space Store Settings | **1335**
- Installing and Upgrading Junos Space Applications from Junos Space Store | **1336**

Running Applications in Separate Server Instances | **1338**

- Adding a Server Group | **1339**
- Adding a Server to a Server Group | **1340**
- Starting Servers in a Server Group | **1341**
- Stopping Servers in a Server Group | **1341**
- Removing a Server Group | **1342**
- Moving an Application to a Different Server Group | **1342**

Managing Junos Space Applications | **1343**

- Viewing Detailed Information About Junos Space Platform and Applications | **1344**
- Performing Actions on Junos Space Platform and Applications | **1344**

Modifying Settings of Junos Space Applications | **1345**

Modifying Junos Space Network Management Platform Settings | **1346**

Managing File Integrity Check | **1367**

- Configuring File Integrity Check | **1367**
- Manually Checking File Integrity | **1368**

Starting, Stopping, and Restarting Services | **1369**

Adding a Junos Space Application | **1372**

Uploading the Junos Space Application | **1372**

Installing the Uploaded Junos Space Application | **1374**

Upgrading a Junos Space Application | **1376**

Upgrading Junos Space Network Management Platform | **1378**

Synchronizing Time Across Junos Space Nodes | **1384**

Upgrading to Junos Space Network Management Platform Release 16.1R1 | **1387**

Before You Begin | **1388**

Downloading and Installing the Junos Space Platform 15.2R2 Patch | **1389**

Executing the Data Back Up Procedure | **1390**

Validating the Backup File | **1394**

Installing Junos Space Platform Release 16.1R1 as a Standalone Node or the First Node of the Fabric and Restoring the Backed-Up Data | **1396**

Rolling Back to Junos Space Platform Release 15.2R2 if Upgrade Fails | **1399**

Installing Junos Space Platform Release 16.1R1 on the Remaining Nodes of the Fabric | **1403**

Configuring Device Communication | **1404**

Managing Disaster Recovery Configuration after Upgrade to 16.1 | **1405**

Appendix: Sample Data of Time Taken for Backup and Restore While Upgrading to Junos Space Platform Release 16.1R1 | **1405**

Uninstalling a Junos Space Application | **1406**

Managing Troubleshooting Log Files | 1408

System Status Log File Overview | **1408**

System Status Log File | **1408**

Customizing Status Log File Content | **1409**

Downloading System Log Files for a Junos Space Appliance | **1409**

Customizing Log Files to Download | **1410**

Customizing Node System Status Log Checking | **1410**

Customizing Node Log Files to Download | **1412**

Configuring JBoss and OpenNMS Logs in Junos Space | **1412**

Generating JBoss Thread Dump for Junos Space Nodes | **1414**

Downloading the Troubleshooting Log File in Server Mode | **1417**

Downloading the Troubleshooting Log File in Maintenance Mode | **1420**

Downloading Troubleshooting System Log Files Through the Junos Space CLI | **1421**

- Downloading a System Log File by Using a USB Device | **1421**
- Downloading System Log File by Using SCP | **1423**

Managing Certificates | 1426

Certificate Management Overview | **1426**

- Authentication Modes Workflow | **1427**
- Custom Junos Space Server Certificates | **1429**
- Certificate Attributes | **1429**
- User Certificates | **1431**
- CA Certificates and CRLs | **1432**
- Changing the User Authentication Mode | **1432**
- Certificate Expiry | **1432**
- Invalid User Certificates | **1433**

Changing User Authentication Modes | **1434**

- Changing the User Authentication Mode from Password-Based to Complete Certificate-Based from the User Interface | **1435**
- Changing the User Authentication Mode from Complete Certificate-Based to Certificate Parameter–Based from the User Interface | **1437**
- Changing the User Authentication Mode from Certificate Parameter–Based to Complete Certificate-Based from the User Interface | **1439**
- Changing the User Authentication Mode to Password-Based from the User Interface | **1440**
- Changing the User Authentication Mode to Password-Based from the CLI | **1440**

Installing a Custom SSL Certificate on the Junos Space Server | **1441**

- Installing an X.509 Junos Space Server Certificate | **1441**
- Installing a Junos Space Server Certificate in the PKCS #12 Format | **1443**
- Reverting to the Default Junos Space Server SSL Certificate | **1444**

Uploading a User Certificate | **1445**

- Uploading a User Certificate for a New User | **1445**
- Uploading a User Certificate for an Existing User | **1446**
- Uploading Your User Certificate | **1447**

Uploading a CA Certificate and Certificate Revocation List | **1448**

- Uploading a CA Certificate | **1448**
- Uploading a Certification Revocation List | **1449**
- Deleting CA Certificates or Certificate Revocation Lists | **1449**

Deleting a CA Certificate or Certificate Revocation List | **1450**

Adding and Activating X.509 Certificate Parameters for X.509 Certificate Parameter Authentication | **1451**

- Adding X.509 Certificate Parameters for X.509 Certificate Parameter Authentication | **1451**
- Activating an X.509 Certificate Parameter | **1453**

Modifying an X.509 Certificate Parameter | **1454**

Deleting X.509 Certificate Parameters | **1455**

Configuring Authentication Servers | 1457

Remote Authentication Overview | **1457**

Junos Space Authentication Modes Overview | **1458**

- Local Authentication | **1459**
- Remote Authentication | **1459**
- Remote-Local Authentication | **1460**

Junos Space Login Behavior with Remote Authentication Enabled | **1461**

Managing Remote Authentication Servers | **1467**

Creating a Remote Authentication Server | **1468**

Modifying Authentication Settings | **1471**

Configuring a RADIUS Server for Authentication and Authorization | **1473**

Configuring a TACACS+ Server for Authentication and Authorization | **1475**

Managing SMTP Servers | 1477

Managing SMTP Servers | **1477**

Adding an SMTP Server | **1478**

Email Listeners | 1481

Email Listeners Overview | **1481**

Adding Users to the Email Listeners List | **1482**

Modifying Users in the Email Listeners List | **1483**

Deleting Users from the Email Listeners List | **1484**

Managing Git Repositories | 1485

Git Repositories in Junos Space Overview | **1485**

Managing Git Repositories in Junos Space | **1486**

- Adding Git Repositories to Junos Space | **1487**
- Modifying Git Repositories in Junos Space | **1488**
- Deleting Git Repositories from Junos Space | **1488**
- Setting the Active Git Repository | **1489**
- Testing the Connection to the Git Repository | **1490**

Viewing Git Repositories in Junos Space | **1490**

Audit Log Forwarding | 1492

Audit Log Forwarding in Junos Space Overview | **1492**

Viewing Audit Log Forwarding Criterion | **1493**

Adding Audit Log Forwarding Criterion | **1496**

Modifying Audit Log Forwarding Criterion | **1497**

Deleting Audit Log Forwarding Criterion | **1498**

Enabling Audit Log Forwarding Criterion | **1499**

Testing the System Log Server Connection for Audit Log Forwarding | **1500**

Configuring a Proxy Server | 1502

Configuring Proxy Server Settings | **1502**

Managing Tags | 1505

Tags Overview | **1506**

- My Favorite Private Tag | **1507**
- Device Tags | **1507**

Creating a Tag | **1507**

Managing Tags | **1512**

Managing Hierarchical Tags | **1513**

- Using the Tag Hierarchy Pane | **1514**
  - Using the Tag Action Bar | **1515**
  - Using the Shortcut Menu | **1516**
  - Using Drag-and-Drop | **1518**
  - Using the Quick Info Tool Tip | **1519**

Browsing Tagged Objects | 1519

Viewing All Tags | 1519

Adding a Child Tag | 1520

Deleting a Tag | 1520

Using Notification | 1520

Using the Tabular View Pane | 1520

Sharing a Tag | 1521

Renaming Tags | 1522

Deleting Tags | 1523

Tagging an Object | 1526

Untagging Objects | 1527

Filtering the Inventory by Using Tags | 1528

Viewing Tagged Objects | 1529

Viewing Tags for a Managed Object | 1532

Exporting Tags from Junos Space Network Management Platform | 1533

Managing DMI Schemas | 1534

DMI Schema Management Overview | 1534

Viewing and Managing DMI Schemas | 1536

Viewing Missing DMI Schemas | 1538

Setting a Default DMI Schema | 1540

Configuring Access to Juniper Networks DMI Schema Repository by Using the Configure SVN Repository Action | 1541

Adding Missing DMI Schemas or Updating Outdated DMI Schemas in Junos Space Network Management Platform | 1543

Adding Missing DMI Schemas by Using the View/Install Missing Schema Action | 1543

Adding Missing DMI Schemas or Updating Outdated DMI Schemas by Using the Get Latest Action | 1544

Adding Missing DMI Schemas or Updating Outdated DMI Schemas by Using REST APIs | 1544

Adding Missing DMI Schemas or Updating Outdated DMI Schemas by Using the Update Schema Menu | 1548

Creating a Compressed TAR File for Updating DMI Schema | 1553

Creating a Compressed Tar File on Linux | 1553

Creating a Compressed Tar File on Microsoft Windows | 1554

Schemas Available in Junos Space Platform | 1556

Viewing and Deleting Unused DMI Schemas | **1557**

Managing Hardware Catalog | 1559

Hardware Catalog Overview | **1559**

Viewing Information About Hardware Catalog | **1561**

Configuring Access to Juniper Networks Subversion Repository for Downloading Hardware Catalog | **1561**

Uploading Hardware Catalog to Junos Space Network Management Platform | **1563**

- Updating Hardware Catalog in Junos Space Platform by Using the Get Latest Action | **1563**
- Uploading Hardware Catalog to Junos Space Platform by Using the Import Option | **1564**

Managing the Purging Policy | 1566

Junos Space Purging Policy and Purging Categories Overview | **1566**

Viewing the Junos Space Purging Policy and Purging Criteria | **1567**

Modifying the Purging Policy and Purging Criteria and Setting the Policy Status | **1569**

- Modifying the Purging Trigger Conditions | **1570**
- Modifying the Purging Criteria and Enabling or Disabling a Policy | **1572**

Guide 4 Monitoring and Troubleshooting Guide

13 **Overview**

Overview | 1576

Monitoring Network Devices and Troubleshooting Software Issues with Junos Space Network Management Platform | **1576**

- Systems of Record | **1577**
- System Snapshot | **1577**
- Backup and Restore | **1578**
- Maintenance Mode | **1578**
- Audit Logs | **1578**
- Jobs | **1579**
- Secure Console | **1579**
- Looking Glass | **1579**
- Reports | **1579**

Junos Space Debug Utilities | **1580**

Overall System Condition and Fabric Load History Overview | **1580**

Overall System Condition | **1580**

Fabric Load History | **1582**

Active Users History | **1582**

Junos Space Network Management Platform Widgets | **1583**

Devices | **1583**

Device Templates | **1584**

CLI Configlets | **1584**

Images and Scripts | **1584**

Reports | **1584**

Network Monitoring | **1585**

Configuration Files | **1585**

Jobs | **1585**

Role Based Access Control | **1586**

Audit Logs | **1586**

Administration | **1586**

14 **Log Files and Debug Utilities**

Troubleshooting Junos Space Network Management Platform Issues by Using Log Files | 1589

System Status Log File Overview | **1589**

System Status Log File | **1589**

Customizing Status Log File Content | **1590**

Downloading System Log Files for a Junos Space Appliance | **1590**

Customizing Log Files to Download | **1591**

Junos Space Network Management Platform Log Files Overview | **1591**

Apache Web Server Log Files | **1592**

JBoss Application Server Log Files | **1592**

MySQL Database Log Files | **1594**

Node Management Agent Log Files | **1594**

Troubleshooting Log File Overview | **1595**

Downloading the Troubleshooting Log File in Server Mode | **1596**

Downloading the Troubleshooting Log File in Maintenance Mode | **1599**

Downloading Troubleshooting System Log Files Through the Junos Space CLI | **1600**

- Downloading a System Log File by Using a USB Device | **1600**
- Downloading System Log File by Using SCP | **1602**

Customizing Node System Status Log Checking | **1605**

Customizing Node Log Files to Download | **1606**

Troubleshooting Network Devices by Using Junos Space Debug Utilties | 1607

Junos Space Debug Utilities Overview | **1607**

- Device-Connection Debug Scripts | **1608**
  - getDeviceInfo.sh | **1608**
  - DeviceDebugInfoCollector.sh | **1608**
  - getAllDeviceInfo.sh | **1608**
  - cleanupEditChannel.sh | **1609**
- Device Import Scripts and Java Applications | **1609**
  - cleanupDeviceImportTables.sh | **1609**
  - DB-blob-reader.jar | **1609**
- Job Management Scripts and Java Applications | **1610**
  - SystemLoadViewer.sh | **1610**
  - getJobThreadSump.sh | **1610**
  - JobInfoCollector.jar | **1610**
- HornetQ Scripts | **1611**
  - HornetQInfoProvider.sh | **1611**
  - HQMessageViewer.sh | **1611**

Executing Device-Connection Debug Scripts | **1611**

- Executing the Script to Collect Device-Connection Information | **1612**
- Executing the Script to Collect Device Debug Information | **1614**
- Executing the Script to Unlock the Device Configuration | **1619**
- Executing the Script to Collect Node-Connection Information | **1620**

Executing Device Import Detail Script and Java Application | **1626**

- Executing the Script to Delete Data from Device Import Tables | **1626**
- Executing the Java Application to View Device XML | **1627**

Executing Job Management Scripts and Java Applications | 1629

Executing the Java Application to Collect Job Information | 1629

Executing the Script to View the Stack Trace of a Job | 1633

Executing the Script to View Job Information on Nodes | 1634

Executing HornetQ Scripts | 1640

Executing the HornetQ Script to View all JBoss Queues | 1640

Executing the HornetQ Script to List of Messages in a JBoss Queue | 1642

15 Troubleshooting Junos Space Platform Issues

Troubleshooting Login–Related Issues | 1646

Troubleshooting the Not Able to Log In from the Junos Space Login Page Issue | 1646

Troubleshooting Device Management–Related Issues | 1648

Troubleshooting Device Discovery Failure | 1648

Troubleshooting Device Data Collection Issue | 1649

Troubleshooting Devices Discovered Twice Using the Device Discovery Workflow | 1650

Troubleshooting Network Monitoring–Related Issues | 1651

Troubleshooting the Network Monitoring Page Is Not Available Issue | 1651

Troubleshooting DMI Schema–Related Issues | 1652

Troubleshooting the Nondisplay of the DMI Schema Tree Issue | 1652

Guide 5 High Availability and Disaster Recovery Guide

16 High Availability

Overview | 1656

Junos Space High Availability Overview | 1656

High Availability Characteristics of Junos Space Appliances | 1658

Understanding the High Availability Software Architecture | 1659

Junos Space High Availability Software Architecture Overview | 1659

Junos Space Software Architecture | 1660

Load-Balancing Architecture | 1661

Database Architecture | 1661

Inter-Node Communication Among Nodes in a Junos Space Cluster | **1662**

Software Components for Junos Space Nodes | **1663**

Understanding the Junos Space Cluster (Fabric) Architecture | 1666

Understanding the Logical Clusters Within a Junos Space Cluster | **1666**

Apache Load-Balancer Cluster | **1667**

JBoss Cluster | **1668**

MySQL Cluster | **1669**

Cassandra Cluster | **1671**

Understanding Virtual IP Availability Within a Junos Space Cluster | **1673**

Understanding High Availability Nodes in a Cluster | **1674**

Understanding High Availability Management of DMI Connections | **1676**

High Availability for Network Monitoring | **1677**

High-Availability Fabric without FMPM Nodes | **1677**

High-Availability Fabric with FMPM Nodes | **1678**

Understanding How Devices Are Configured to Send SNMP Traps to Junos Space | **1679**

Configuring High Availability Overview | 1681

Configuring the Junos Space Cluster for High Availability Overview | **1681**

Requirements | **1681**

Preparation | **1682**

Configuring the First Node in the Cluster | **1684**

Adding a Second Node to the Cluster | **1685**

Adding Additional Nodes to a Cluster | **1685**

Configuring FMPM Nodes | **1686**

Removing Nodes from a Cluster | **1686**

High Availability Failover Scenarios | 1687

Understanding High-Availability Failover Scenarios | **1687**

Active VIP Node Crashes | **1688**

Standby VIP Node Crashes | **1688**

eth0 on the Active VIP Node Goes Down | **1689**

eth0 on the Standby VIP Node Goes Down | **1690**

A Non-VIP Node Crashes | **1690**

eth0 on a Non-VIP Node Goes Down | **1690**

eth3 on a Non-VIP Node Goes Down | **1691**

eth3 on the Active VIP Node Goes Down | **1691**

JBoss Server on a Node Goes Down | **1692**

MySQL Server on the Active VIP Node Goes Down | **1693**

MySQL Server on the Standby VIP Node Goes Down | **1693**

Primary Database Node Crashes | **1694**

Secondary Database Node Crashes | **1694**

MySQL Server on the Primary Database Node Goes Down | **1694**

MySQL Server on the Secondary Database Node Goes Down | **1695**

Apache HTTP Server on the Active VIP Node Goes Down | **1695**

Apache HTTP Server on the Standby VIP Node Goes Down | **1696**

Dedicated Cassandra Node Crashes | **1696**

Cassandra Service on a JBoss Node Goes Down | **1696**

17 **Disaster Recovery**

Disaster Recovery Solution | 1699

Disaster Recovery Overview | **1699**

Disaster Recovery Solution | **1700**

Prerequisites to Configure Disaster Recovery | **1702**

Connectivity Requirements to Configure Disaster Recovery | **1703**

Disaster Recovery Watchdog | **1703**

heartbeat | **1704**

mysqlMonitor | **1704**

pgsqlMonitor | **1704**

fileMonitor | **1705**

arbiterMonitor | **1705**

configMonitor | **1705**

serviceMonitor | **1705**

notification | **1705**

Failure Detection by Using the Device Arbitration Algorithm | **1706**

Failure Detection by Using the Custom Failure-Detection Scripts | **1707**

Steps to Configure Disaster Recovery | **1718**

Disaster Recovery Commands | **1719**

Understanding the Normal Operation of Active and Standby Sites | **1723**

Understanding Disaster Recovery Failure Scenarios | **1724**

Active Site (site1) Goes Down Due to a Disaster or Is Powered Down | **1725**

Detection | **1725**

Impact | **1725**

Recovery | **1725**

No Connectivity Between the Active and Standby Sites and Both Sites Lose Connectivity with Arbiter Devices | **1725**

Detection | **1725**

Impact | **1726**

Recovery | **1726**

No Connectivity Between the Active and Standby Sites | **1726**

Detection | **1726**

Impact | **1726**

Recovery | **1726**

No Connectivity Between the Active and Standby Sites and the Active Site (site1) Loses Connectivity with Arbiter Devices | **1727**

Detection | **1727**

Impact | **1727**

Recovery | **1727**

No Connectivity Between the Active and Standby Sites and the Standby Site (site2) Loses Connectivity With Arbiter Devices | **1727**

Detection | **1727**

Impact | **1728**

Recovery | **1728**

Standby Site (site2) Goes Down Due to Disaster or Is Powered Down | **1728**

Detection | **1728**

Impact | **1728**

Recovery | **1728**

No Connectivity Between the Active Site (site1) and Arbiter Devices | **1729**

Detection | **1729**

Impact | **1729**

Recovery | **1729**

No Connectivity Between the Standby Site (site2) and Arbiter Devices | **1729**

Detection | **1729**

Impact | **1729**

Recovery | **1729**

Understanding How the Standby Site Becomes Operational When the Active Site Goes Down | **1730**

Configuring the Disaster Recovery Process | 1731

Configuring the Disaster Recovery Process Between an Active and a Standby Site | **1731**

Configuring Disaster Recovery at the Active Site | **1732**

Configuring Disaster Recovery at the Standby Site | **1737**

Starting the Disaster Recovery Process | **1741**

Verifying the Status of the Disaster Recovery Process | **1743**

Stopping the Disaster Recovery Process on Junos Space Network Management Platform Release 14.1R3 and Earlier | **1743**

Stopping the Backup Process at the Active Site | **1743**

Stopping Collecting Backups from the Active Site | **1745**

Managing the Disaster Recovery Solution | 1747

Checking the Status of the Disaster Recovery Configuration | **1747**

Viewing the Disaster Recovery Configuration and Status of Watchdog Services | **1752**

Modifying the Disaster Recovery Configuration | **1754**

Modifying Applications and Nodes on a Disaster Recovery Setup | **1765**

Upgrading the Junos Space Network Management Platform Software | **1767**

Upgrading to Junos Space Network Management Platform Release 16.1R1 | **1772**

Installing a Junos Space Application | **1773**

Upgrading a Junos Space Application | **1774**

Uninstalling a Junos Space Application | **1775**

Adding or Removing a JBoss Node | **1776**

Adding or Removing a Dedicated Junos Space Node | **1778**

Manually Failing Over the Network Management Services to the Standby Site | **1780**

Stopping the Disaster Recovery Process | **1784**

Resetting the Disaster Recovery Configuration | **1786**

Upgrading Junos Space Network Management Platform with Disaster Recovery Enabled | 1789

Upgrade Procedure | **1789**

1. Back up the Current Disaster Recovery Configuration | **1790**

2. Reset the Disaster Recovery Configuration | **1790**

3. Upgrade the Junos Space Network Management Platform and Application | **1790**

4. Configure and Perform Disaster Recovery | **1793**

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | xlvii
- Supported Platforms | xlvii
- Documentation Conventions | xlvii
- Documentation Feedback | l
- Requesting Technical Support | l

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at https://www.juniper.net/documentation/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at https://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

Documentation Conventions

Table 1 defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		

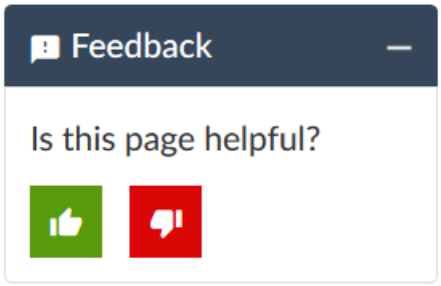
Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:



  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Create a service request online: https://myjuniper.juniper.net

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://entitlementsearch.juniper.net/entitlementsearch/

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit https://myjuniper.juniper.net.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see https://support.juniper.net/support/requesting-support/.

Getting Started Guide

CHAPTER 1

Junos Space Fabric Deployment

Junos Space Fabric Architecture | 54

Junos Space Fabric Deployment Overview | 54

Junos Space Fabric Architecture

To support the rapid growth in network size, Junos Space is designed to be highly scalable. You can cluster multiple Junos Space appliances to create a single management fabric, which is accessible from a single virtual IP (VIP) address.

All graphical user interface (GUI) and northbound interface (NBI) clients use the Junos Space VIP address to connect to the Junos Space fabric. The fabric incorporates a front-end load balancer that distributes client sessions across all the active Junos Space nodes within the fabric. You can increase or decrease the fabric by simply adding or deleting nodes to or from the Junos Space Network Management Platform user interface, and the Junos Space system automatically starts applications and services on the active nodes. Each node in the cluster is fully utilized and all nodes work together to provide automated resource management and service availability.

A Junos Space fabric architecture comprising multiple appliances eliminates any single point of failure. When a node in the fabric goes down, all client sessions and device connections currently served by that node are automatically migrated to the active nodes in the fabric without any user-initiated action.

RELATED DOCUMENTATION

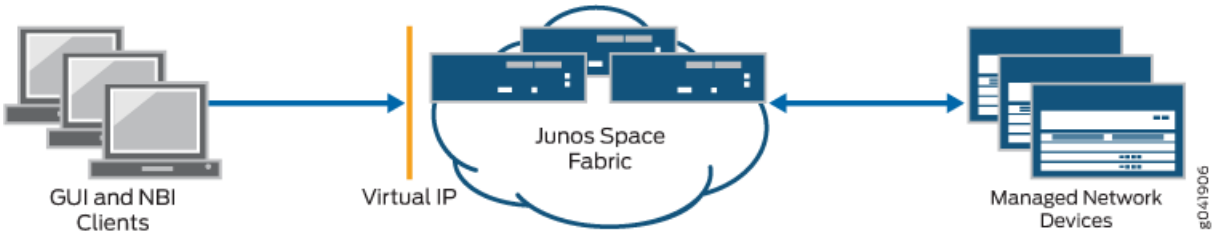
Junos Space Fabric Deployment Overview | 54

Junos Space Fabric Deployment Overview

You can install and deploy Junos Space Hardware Appliances (JA2500), Junos Space Virtual Appliances, or both to form a fabric. Each appliance in the fabric is called a *node*. All nodes in the fabric work together as a cluster of Junos Space instances running in active-active configuration (that is, all nodes are active in the cluster).

Figure 1 displays how a Junos Space fabric employs a software load balancer to distribute HTTP sessions across the nodes to ensure that the load presented by the Junos Space Network Management Platform user interface and NBI clients is equally distributed within the fabric.

Figure 1: Clients Using a Single Virtual IP Address to Access the Junos Space Fabric



A Junos Space fabric of appliances provides scalability and ensures high availability of your management platform. The fabric provides an N+1 redundancy solution where the failure of a single node in the fabric does not affect the functioning of the fabric. When a node in the fabric fails, the sessions of the clients accessing Junos Space from the user interface automatically migrate away from the failed node. Similarly, managed devices that were connected to the failed node are automatically reconnected with another functioning node in the fabric.

Deploying a Junos Space Hardware Appliance

When you power on the Junos Space Hardware Appliance and log in to the CLI console, you can view a menu-driven command-line interface to specify the initial configuration of the appliance.

You need to specify the following parameters:

- IP address and subnet mask for the “eth0” interface
- Virtual IP address (when you configure the first node in the cluster) to access the Junos Space user interface from Web browsers. The IP address should be in the same subnet as the IP address assigned to the “eth0” interface.
- IP address of the default gateway
- IP address of the name server
- IP address and subnet mask for the “eth3” interface if you choose to manage devices on a different Ethernet interface (see Figure 3).
- Whether the appliance will be added to an existing cluster. Choose “n” to add the first node to a new cluster and choose “y” to add subsequent nodes to the cluster.
- NTP server settings with which to synchronize the appliance’s time
- Maintenance mode user ID and password

> **NOTE:** Ensure that you remember the Maintenance mode user ID and password. These details are required when you upgrade software and restore databases.

Refer to the *JA2500 Junos Space Appliance Quick Start Guide* for detailed instructions on how to configure the hardware appliance during initial deployment.

Deploying a Junos Space Virtual Appliance

The Junos Space Virtual Appliance is stored in the open virtual appliance (OVA) format and is packaged as an ***.ova** file, which is a single folder that contains all the files of the Junos Space Virtual Appliance. OVA is not a bootable format and you must deploy each Junos Space Virtual Appliance to a hosted ESX or ESXi server before you can run the Junos Space Virtual Appliance.

You can deploy a Junos Space Virtual Appliance on a VMware ESX server version 4.0 or later or VMware ESXi server version 4.0 or later. After the Junos Space Virtual Appliance is deployed, you can use the VMware vSphere client that is connected to the VMware ESX (or VMware ESXi) server to configure the Junos Space Virtual Appliance. You can deploy Junos Space Virtual Appliance 14.1R2.0 and later on qemu-kvm Release 0.12.1.2-2/448.el6. You must deploy and configure the Junos Space Virtual Appliance on a KVM server by using the Virtual Machine Manager (VMM) client.

The CPU, RAM, and disk space provided by the VMware ESX server or KVM server must meet or exceed the documented CPU, RAM, and disk space requirements for deploying a Junos Space Virtual Appliance. In addition, we recommend that, for a multinode fabric, you deploy the first and second virtual appliances on separate servers to ensure failover support.

The distributed Junos Space Virtual Appliance files are created with 135 GB of disk space. If you create a multinode cluster, ensure that the first and second nodes that you deploy should contain the same amount of disk space. When the disk resources are used beyond 80% capacity, add sufficient disk space (more than 10 GB) to the disk partitions.

When you log in to the console of the VMware vSphere client or VMM client, you need to specify the same parameters used to deploy a hardware appliance. Refer to the *Junos Space Virtual Appliance Deployment and Configuration Guide* for detailed instructions on how to configure the virtual appliance during initial deployment.

Basic Requirements for a Fabric Deployment

When you deploy multiple appliances to create a Junos Space fabric, each appliance in the fabric uses the eth0 interface for all internode communication within the fabric. On each appliance, you can choose to use a separate interface (eth3) for all communication between the appliance and managed devices, as shown in Figure 3.

The following are required when you deploy a Junos Space fabric:

- You must be able to ping the default gateway IP address, or else the fabric will not form correctly.
- The IP addresses assigned to the eth0 interface on the first two appliances in the fabric must be in the same subnet.
- The virtual IP address configured on the first appliance in the fabric must be in the same subnet as the eth0 interface on the first two appliances.
- Multicast packets must be routable among all nodes because JBoss cluster-member discovery uses multicast routing.
- If you are deploying a fabric of virtual appliances, we recommend that the first and second appliances added to the fabric be hosted on a separate VMware ESX or ESXI server to ensure failover support.
- All appliances in the fabric must use the same external NTP source to ensure consistent time setting across all appliances in the fabric You must specify the NTP source on each appliance before adding the appliance to the fabric.
- All nodes in the fabric are running the same version of the software.

Configuring Network Connectivity for a Junos Space Fabric

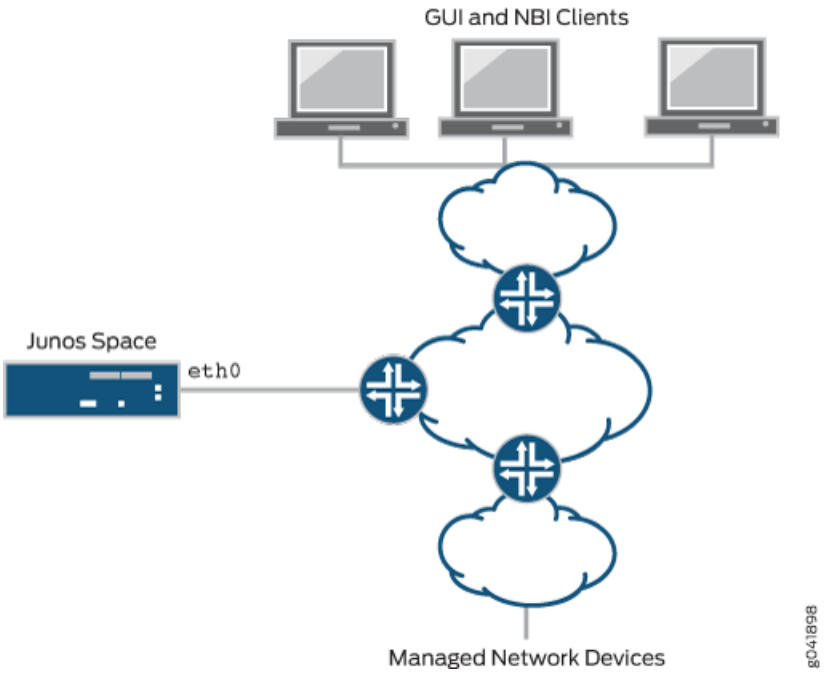
A Junos Space appliance (hardware or virtual) has four RJ45 10/100/1000 Ethernet interfaces that are named eth0, eth1, eth2, and eth3. When deploying the appliance, you need to ensure that it has IP connectivity with the following:

- Devices in your managed network
- Desktops, laptops, and workstations from which Junos Space users access the Junos Space user interface as well as external systems hosting NBI clients
- Other appliances that form a Junos Space fabric along with this appliance

Junos Space allows you to use two of the four Ethernet interfaces: eth0 and eth3. The other two Ethernet interfaces are reserved for future use. You can choose one of the following two options for configuring interfaces for IP connectivity:

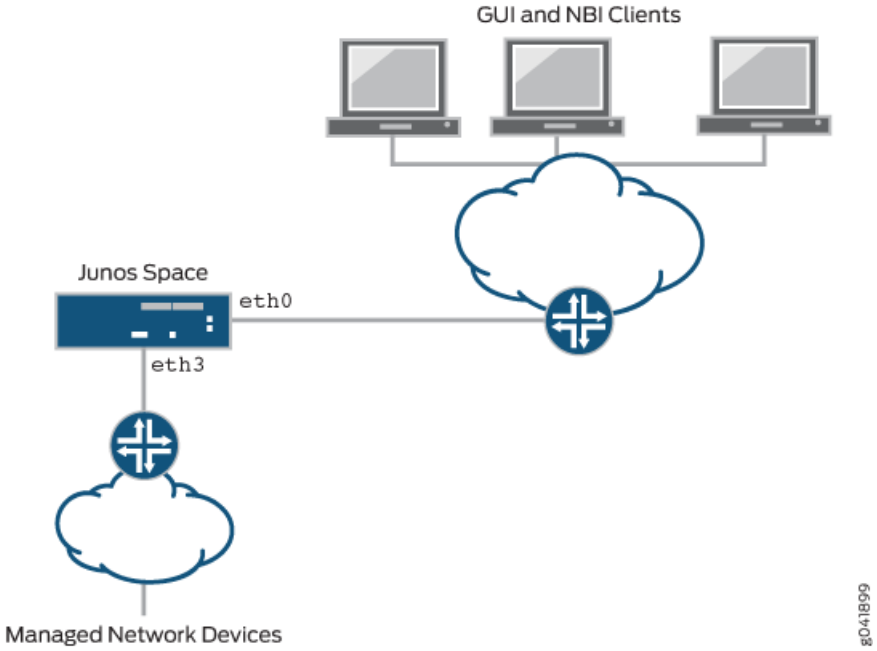
- Use the eth0 interface for all network connectivity of the appliance, as shown in Figure 2.

Figure 2: Using a Single Ethernet Interface for All IP Connectivity



- Use the eth0 interface for network connectivity with Junos Space user interface clients and other appliances in the same fabric, and use the eth3 interface for network connectivity with managed devices, as shown in Figure 3.

Figure 3: Using Two Interfaces for IP Connectivity



Adding Nodes to a Junos Space Fabric

You must be assigned the System Administrator user role to be able to add nodes to a Junos Space fabric. You add nodes to a Junos Space fabric from the **Add Fabric Node** page (**Network Management Platform > Administration > Fabric > Add Fabric Node**). To add a node to a fabric, you specify the IP address assigned to the eth0 interface of the new node, a name for the new node, and (optionally) a scheduled date and time to add the node to the fabric. Junos Space software automatically handles all necessary configuration changes to add the node to the fabric. After the new node is added to the fabric, you can monitor the status of the node from the **Fabric** page (**Network Management Platform > Administration > Fabric**).

For complete information about adding nodes to a fabric, see the "Adding a Node to an Existing Junos Space Fabric" on page 1176 topic (in the *Junos Space Network Management Platform Workspaces User Guide*).

RELATED DOCUMENTATION

Junos Space Fabric Architecture | **54**

Installing and Upgrading Junos Space Software Overview | **61**

2

CHAPTER

Junos Space System Administration

Installing and Upgrading Junos Space Software Overview | **61**

Junos Space Applications Supported on the Junos Space Platform | **65**

Junos Space License Installation Overview | **66**

DMI Schema Overview | **67**

Backing Up the Junos Space Platform Database | **68**

Configuring User Access Controls Overview | **69**

Installing and Upgrading Junos Space Software Overview

IN THIS SECTION

- Installing Junos Space Applications | 61
- Upgrading Junos Space Applications | 62
- Upgrading Junos Space Network Management Platform | 63
- Uninstalling Junos Space Applications | 64

The following sections describe the primary software administration tasks for the Junos Space Network Management Platform and Junos Space applications:

CAUTION: Do not modify the filename of the software image that you download from the Juniper Networks support site. If you modify the filename, the installation or upgrade fails.

NOTE: Juniper Networks devices require a license to activate the feature. To understand more about Junos Space Network Management Platform Licenses, see, Licenses for Network Management. Please refer to the Licensing Guide for general information about License Management. Please refer to the product Data Sheets for further details, or contact your Juniper Account Team or Juniper Partner.

Installing Junos Space Applications

Before installing an application, verify that the application is compatible with the Junos Space Network Management Platform. For more information about application compatibility, see the Knowledge Base article KB27572 at https://kb.juniper.net/InfoCenter/index?page=content&id=KB27572.

You can upload an application image file to Junos Space from the **Add Application** page (**Administration > Applications > Add Application**). You can upload an application image file by using HTTP (**Upload via HTTP**) option or Secure Copy Protocol (SCP) (**Upload via SCP**) option. We recommend that you upload the file by using SCP, which initiates a direct transfer from an SCP server to Junos Space and is performed as a back-end job. If you choose to upload the file using SCP, you must first make the image file available on an SCP server that Junos Space can access. You must also provide the IP address of the SCP server and the login credentials needed to access this SCP server. The main advantage of using SCP is that your user interface is not blocked while the file transfer is in progress, and you can monitor the progress of the file transfer from the **Jobs** workspace.

> **NOTE:** A Junos Space node can also be used as an SCP server. To do this, copy the application image file (using SCP or SSH FTP [SFTP]) to the **/tmp/** directory on the Junos Space node, and in the **Upload Software via SCP** dialog box specify the credentials (username and password), the IP address of the Junos Space node, the CLI credentials, and the file path for the software image.

After the image file for the application is uploaded successfully, you can view the application from the **Add Application** page. You can then select the application file and click the **Install** button to install the application. The application installation process does not cause any downtime for the Junos Space Network Management Platform or any applications installed on Junos Space. Junos Space Network Management Platform ensures that the application is installed on all nodes in the Junos Space fabric and access to the application is load balanced across all nodes in the Junos Space fabric.

For more information about installing Junos Space applications, see the "Managing Junos Space Applications Overview" on page 1328 topic (in the *Junos Space Network Management Platform Workspaces User Guide*).

Upgrading Junos Space Applications

You can easily upgrade a Junos Space application from the Junos Space Platform UI. You must download the image file for the new version of the application, navigate to the **Applications** page (**Administration > Applications**), right-click the application that you want to upgrade, and select **Upgrade Application** to upload the image file into Junos Space through HTTP or SCP. We recommend that you use the SCP option, which initiates a direct transfer from an SCP server to Junos Space. After the image file is uploaded, select the uploaded file and click the **Upgrade** button to start the upgrade process. If you perform the upgrade by using SCP, then the upgrade process is executed as a back-end job by the Junos Space Network Management Platform, and you can monitor the progress of the upgrade from the **Jobs** workspace. An application upgrade does not cause downtime for the Junos Space Network Management Platform or other applications that are hosted by Junos Space.

For more information about upgrading Junos Space applications, see the "Managing Junos Space Applications Overview" on page 1328 topic (in the *Junos Space Network Management Platform Workspaces User Guide*).

Upgrading Junos Space Network Management Platform

Juniper Networks typically produces two major releases of the Junos Space Network Management Platform per year. In addition, one or more patch releases might accompany each major release. You can upgrade to a newer Junos Space Platform release by performing a few simple steps from the user interface in your current Junos Space Platform.

NOTE: If you are upgrading to Junos Space Platform Release 16.1R1 or 16.1R2, follow the procedure outlined in the topic "Upgrading to Junos Space Network Management Platform Release 16.1R1" on page 1387 in the *Workspaces User Guide*.

WARNING: Upgrading to a new Junos Space Network Management Platform version might disable functionality and the ability to use the installed Junos Space applications. Before you upgrade the Junos Space Network Management Platform, take inventory of the applications installed. If Junos Space Network Management Platform is upgraded and a compatible application is not available, the installed application is deactivated and cannot be used until a compatible application has been released.

If you are upgrading Junos Space Platform to releases other than Junos Space Platform Release 16.1R1, the workflow for performing the upgrade is similar to that of installing an application. After you download the required image file, (**.img** extension) from the Juniper Networks software download site, navigate to the **Applications** page (**Administration > Applications**), right-click the image file, and select **Upgrade Platform** to upload the image file into Junos Space through HTTP or SCP. We recommend that you use the SCP option, which initiates a direct transfer from an SCP server to Junos Space and is performed as a back-end job. If you choose the SCP option, you must first make the image file available on an SCP server that Junos Space can access. After the image file is uploaded, select the uploaded file, and click the **Upgrade** button to start the upgrade process. The Network Management Platform upgrade forces the system into Maintenance mode, which requires that you enter the Maintenance mode username and password to proceed with the upgrade.

During the Junos Space Network Management Platform upgrade process, all the data in the Junos Space database is migrated to the new schema that is part of the new Junos Space release. The upgrade process also seamlessly upgrades all nodes in the fabric. The upgrade process requires a restart of JBoss application servers on all nodes and might also require a reboot of all the nodes if the OS packages are also upgraded. The time required for the upgrade depends on a number of factors, including the amount of data being migrated, the number of nodes in the fabric, and the number of third-party components upgraded. You should expect an average downtime of 30 to 45 minutes for upgrade of a single-node fabric, and approximately 45 to 60 minutes for upgrade of a two-node fabric.

NOTE: You can use this workflow to upgrade to Release 18.1 from Release 17.2 or Release 17.1. If you are upgrading to Release 18.1 from a release earlier than 16.1, you must first upgrade the installation to Release 16.1 and then, upgrade to Release 17.1 or Release 17.2. You must perform multistep upgrades if a direct upgrade is not supported between the version from which you want to upgrade and the version to which you want to upgrade. For detailed information about the releases from which Junos Space Platform can be upgraded, see the *Junos Space Network Management Platform Release Notes*.

Before you upgrade Junos Space Platform to Release 18.1, ensure that the time on all Junos Space nodes is synchronized. For information about synchronizing time on Junos Space nodes, see "Synchronizing Time Across Junos Space Nodes" on page 1384.

For more information about upgrading the Junos Space Network Management Platform, see the "Upgrading Junos Space Network Management Platform Overview" on page 1330 topic in the *Junos Space Network Management Platform Workspaces User Guide*.

Uninstalling Junos Space Applications

To uninstall a Junos Space application, navigate to the **Applications** page (**Administration > Applications**), right-click the application that you want to uninstall, and select **Uninstall Application**. You are prompted to confirm the uninstallation process. Upon confirmation, the uninstallation process for the application is executed as a back-end job by Junos Space. You can monitor the progress of the job from the **Job Management** page (**Jobs > Job Management**). The uninstallation process does not cause downtime for Junos Space Network Management Platform or other applications hosted by Junos Space Network Management Platform.

For more information about uninstalling Junos Space applications, see the "Uninstalling a Junos Space Application" on page 1406 topic in the *Junos Space Network Management Platform Workspaces User Guide*).

RELATED DOCUMENTATION

Junos Space License Installation Overview | 66

Junos Space Applications Supported on the Junos Space Platform | 65

Configuring User Access Controls Overview | 69

Junos Space Applications Supported on the Junos Space Platform

A number of high-level applications are available for Junos Space Network Management Platform. You can install these applications to simplify network operations, scale services, automate support, and open the network to new business opportunities.

The Junos Space Network Management Platform is a multitenant platform that enables you to install hot-pluggable applications. Junos Space automatically deploys the installed applications across the fabric. You can install, upgrade, and remove applications without disrupting or causing any downtime for the Junos Space Network Management Platform or other hosted applications.

The following applications are currently available for Junos Space Network Management Platform:

- Junos Space Log Director–Enables log collection across SRX Series Services Gateways and enables log visualization
- Junos Space Network Director–Enables unified management of Juniper Networks EX Series Ethernet Switches, EX Series Ethernet switches with ELS support, QFX Series switches, QFabric, wireless LAN devices, and VMware vCenter devices in your network
- Junos Space Security Director –Allows you to secure your network by creating and publishing firewall policies, IPsec VPNs, network address translation (NAT) policies, intrusion prevention system (IPS) policies, and application firewalls
- Junos Space Services Activation Director–Collection of the following applications that facilitate automated design and provisioning of Layer 2 VPN and Layer 3 VPN services, configuration of QoS profiles, validation and monitoring of service performance, and management of synchronization:
  - Network Activate
  - Junos Space OAM Insight
  - Junos Space QoS Design
  - Junos Space Transport Activate
  - Junos Space Sync Design
- Junos Space Service Automation–End-to-end solution designed to streamline operations and enable proactive network management for Junos OS devices. The Service Automation solution consists of the following:
  - Junos Space Service Now
  - Junos Space Service Insight

  - Advanced Insight Scripts (AI-Scripts)

- Junos Space Virtual Director–Enables the provisioning, bootstrapping, monitoring, and lifecycle management of a variety of Juniper virtual appliances and related virtual security solutions

> **NOTE:** For information about the Junos Space applications supported for a specific version of the Junos Space Network Management Platform, see the Knowledge Base article KB27572 at https://kb.juniper.net/InfoCenter/index?page=content&id=KB27572.

RELATED DOCUMENTATION

Installing and Upgrading Junos Space Software Overview | 61

Junos Space License Installation Overview

Junos Space Network Management Platform comes with a 60-day full-featured trial license. You must procure and install a valid license during this period to ensure continued operation beyond the trial period.

If you fail to upload a valid license during the 60-day trial period, the Junos Space user interface displays an error message when you log in indicating that the license has expired. Your access is limited to the Licenses page (**Administration > Licenses**) from where you can execute the **Import License** task to enter a valid license.

You can use either of the following options to install a valid license for Junos Space Platform:

- If you plan to use the Junos Space Platform with only the Support Automation applications (Service Now and Service Insight), you can navigate to the **Add Organization** page (**Service Now > Administration > Organizations > Add Organization**) in the Service Now user interface to activate these applications. However, to activate these applications, you must have a valid support contract for your Juniper Networks devices and valid credentials to access the Juniper Support System (JSS) back end.

> **NOTE:** If you choose this option and if you want to use other Junos Space applications beyond the trial period, you must purchase a license for Junos Space Platform (as explained in the bulleted item that follows).

- If you want to use Junos Space applications other than Service Now and Service Insight, or if you do not have a valid support contract for your Juniper Networks devices, you must purchase a license for Junos Space Platform. After you obtain the license file, you can install the license from the **Import License** page (**Administration > Licenses > Import License**). For more information about installing a valid license for Junos Space Platform, see the "Generating and Uploading the Junos Space License Key File" on page 1323 topic (in the *Junos Space Network Management Platform Workspaces User Guide*).

RELATED DOCUMENTATION

Installing and Upgrading Junos Space Software Overview | 61

DMI Schema Overview

Each device type is described by a unique data model that contains all the configuration data for that device. The schemas for this data model list all the possible fields and attributes for a type of device. The newer schemas describe the new features associated with recent device releases.

Junos Space Network Management Platform provides support for managing devices based on Device Management Interface (DMI) schema.

You must load all your device schemas into Junos Space Network Management Platform; otherwise, only a default schema is applied when you try to edit a device configuration using the device configuration edit action in the Devices workspace (as described in "Modifying the Configuration on the Device" on page 322 in the *Junos Space Network Management Platform Workspaces User Guide*).

If the Junos Space Network Management Platform contains exactly the right schema for each of your devices, you can access all the configuration options specific to each device. You can add or update schemas for all Junos Space devices from the Administration workspace (**Administration > DMI Schemas**) workspace. You can use this workspace to check whether a schema for a device is missing. On the Manage DMI Schemas page, in tabular view, the DMI Schema column displays *Need Import* if the Junos OS schema for that particular device OS is not bundled with the Junos Space Network Management Platform. Then you need to download the schema from the Juniper Schema Repository.

For complete information about managing DMI schema , see the "DMI Schema Management Overview" on page 1534 topic (in the *Junos Space Network Management Platform Workspaces User Guide*).

RELATED DOCUMENTATION

Device Management in Junos Space Platform | 79

Backing Up the Junos Space Platform Database

You must back up the Junos Space database regularly so that you are able to roll back the system data to a previously known point. You can create a backup schedule on the **Database Backup and Restore** page in the **Administration** workspace (**Network Management Platform > Administration > Database Backup and Restore**). You can store the backup file on the local file system of the Junos Space appliance, or on a remote server by using the Secure Copy Protocol (SCP).

> **NOTE:** We recommend that you back up files on a remote server because this ensures that the backup files are available even if an error occurs on the appliance. In addition, if you back up files remotely instead of locally, you ensure optimal use of the disk space on the Junos Space appliance.

To perform remote backups, you must set up a remote server that can be accessed through the SCP and that has its IP address and credentials available. We recommend that you have a separate partition on this server to store Junos Space backups and that you provide the full path of this partition in the Junos Space user interface when you set up the backup schedule. You can also specify the start date and time for the first backup, the recurrence interval required (hourly, daily, weekly, monthly, or yearly), and the date and time of the last backup (if required). In most cases, we recommend that you back up the database daily. You can customize the backup frequency based on the needs of your organization and the amount of change that occurs in the network. In addition, you can schedule backups to run automatically when the system usage is low. Creating a backup schedule ensures that database backups occur at the scheduled time and at the scheduled recurrence intervals. You can also perform database backups on demand from the **Database Backup and Restore** page, in the **Administration** workspace (**Network Management Platform > Administration > Database Backup and Restore**), by clearing the check boxes that control the time of occurrence and recurrence intervals.

Whether scheduled or performed on demand, each successful backup generates an entry that is available on the **Database Backup and Restore** page. You can select the database backup entry and select the **Restore From Remote File** action to restore the system data to the selected backup.

> **NOTE:** Performing a database restore action causes a downtime in your Junos Space fabric, which goes into Maintenance mode to restore the database from the chosen backup and then waits for the application servers to be restarted.

For complete information about performing backup and restore operations for the Junos Space Network Management Platform, see the "Backing Up and Restoring the Database Overview" on page 1305 and "Backing

Up the Junos Space Network Management Platform Database" on page 1308 topics (in the *Junos Space Network Management Platform Workspaces User Guide*).

RELATED DOCUMENTATION

Installing and Upgrading Junos Space Software Overview | 61
Junos Space Applications Supported on the Junos Space Platform | 65

Configuring User Access Controls Overview

IN THIS SECTION

- Authentication and Authorization Mode | 71
- Certificate–Based and Certificate Parameter–Based Authentication | 73
- User Roles | 73
- Remote Profiles | 74
- Domains | 75
- User Accounts | 75
- Device Partitions | 76

Junos Space Network Management Platform provides a robust user access control mechanism system that you use to enforce appropriate access policies on the Junos Space system through your Junos Space administrators. In Junos Space, administrators can serve different functional roles. A CLI administrator installs and configures Junos Space appliances. A Maintenance-mode administrator performs system-level tasks, such as troubleshooting and database restoration operations. After the appliances are installed and configured, you can create users and assign roles that allow these users to access the Junos Space Platform workspaces and manage the applications, users, devices, services, customers, and so forth.

Table 3 shows the Junos Space administrators and the tasks that can be performed.

Table 3: Junos Space Administrators

Junos Space Administrator Function	Description	Tasks

Table 3: Junos Space Administrators *(continued)*

CLI administrator	An administrator responsible for setting up and managing system settings for Junos Space appliances from the serial console
	
	The CLI administrator name is *admin*.
	
	The CLI administrator password can be changed from the console system settings menu.
		• Install and configure basic settings for Junos Space appliances.
		• Change network and system settings for appliances, for example:
		  ◦ Change the CLI administrator password.
		  ◦ Modify routing parameters.
		  ◦ Modify DNS server settings.
		  ◦ Change time zone and NTP server settings.
		  ◦ Expand the VM drive size (Junos Space Virtual Appliances only).
		  ◦ Retrieve log files for troubleshooting.

Maintenance-mode administrator	An administrator responsible for performing system-level maintenance on Junos Space Network Management Platform The Maintenance-mode administrator name is *maintenance*. The Maintenance-mode password is configured from the serial console when you first configure a Junos Space appliance.	• Restore Junos Space Network Management Platform to its previous state by using a database backup file. • Shut down Junos Space nodes by entering Maintenance mode. • Retrieve log files for troubleshooting. • Exit Maintenance mode and explicitly start up the Junos Space system.
Junos Space user interface users	A Junos Space user that is assigned one or more predefined roles. Each role assigned to a user provides specific access and management privileges on the objects (applications, devices, users, jobs, services, and customers) available from a workspace in the Junos Space user interface.	For more information about the predefined roles that can be assigned to a Junos Space user, see "Configuring User Access Controls Overview" on page 69.

You can configure user access control by:

- Deciding how users will be authenticated and authorized to access Junos Space Platform
- Segregating users based on the system functionality they are allowed to access. You can assign a different set of roles to different users. Junos Space Network Management Platform includes more than 25 predefined user roles and allows you to create custom roles that are based on the needs of your organization. When a user logs in to Junos Space, the workspaces that the user can access and the tasks that they can perform are determined by the roles that have been assigned to that particular user account.
- Segregating users based on the domains that they are allowed to access. You can use the Domains feature in Junos Space to assign users and devices to the global domain and create subdomains, and then assign users to one or more of these domains. A domain is a logical grouping of objects, which can include devices, templates, users, and so on. When a user logs in to Junos Space, the set of objects that they are allowed to see is based on the domains to which that user account has been assigned.

  You can use multiple domains to separate large, geographically distant systems into smaller, more manageable sections and control administrative access to individual systems. You can assign domain administrators or users to manage devices and objects that are assigned to their domains. You can design the domain hierarchy in such a way that a user assigned to one domain need not necessarily have access to objects in another domain. You can even restrict users assigned to a domain from viewing objects that are in the parent domain (in Junos Space Release 13.3, from viewing the objects in the global domain).

  For example, a small organization might have only one domain (the global domain) for their entire network, whereas a large, international organization might have several subdomains within the global domain to represent each of its regional office networks across the world.

The following sections describe how to configure a user access control mechanism:

Authentication and Authorization Mode

The first decision to be made is regarding the mode of authentication and authorization that you want. The default mode in Junos Space is local authentication and authorization, which means that you must create user accounts in the Junos Space database with a valid password and assign a set of roles assigned to those accounts. User sessions are authenticated based on this password, and the set of roles assigned to the user account determine the set of tasks the user can perform.

If your organization relies on a set of centralized authentication, authorization, and accounting (AAA) servers, you can configure Junos Space to work with these servers by navigating to the Authentication Servers page in the Administration workspace (**Network Management Platform > Administration**).

NOTE:

- You must have Super Administrator or System Administrator privileges to configure Junos Space to work with these servers.
- You need to know the IP addresses, port numbers, and shared secrets of the remote AAA servers for configuring Junos Space to access them. We recommend that you use the Connection button to test the connection between Junos Space and the AAA server as soon as you add the server in Junos Space. This immediately lets you know whether there is any problem with the configured IP address, port, or credentials.
- You can configure an ordered list of AAA servers. Junos Space contacts them in the order you configured; the second server is contacted only if the first one is unreachable, and so on.
- You can configure RADIUS or TACACS+ servers over Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). You are allowed to have a mix of RADIUS and TACACS+ servers in the ordered list of AAA servers that Junos Space maintains.
- There are two modes of remote authentication and authorization: remote-only and remote-local.
  - *remote-only*—Authentication and authorization are performed by a set of remote AAA servers (RADIUS or TACACS+).
  - *remote-local*—In this case, when a user is not configured on the remote authentication servers, when the servers are unreachable, or when the remote servers deny the user access, then the local password is used if such a local user exists in the Junos Space database.

If you are using remote-only mode, you do not have to create any local user accounts in Junos Space. Instead, you must create user accounts in the AAA servers that you use and associate a remote profile name to each user account. A remote profile is a collection of roles that define the set of functions that a user is allowed to perform in Junos Space. You create the remote profiles in Junos Space. For more information about remote profiles, see "Remote Profiles" on page 74. Remote profile names can be configured as a vendor-specific attribute (VSA) in RADIUS and as an attribute-value pair (AVP) in TACACS+. When an AAA server successfully authenticates a user session, the remote profile name is included in the response message that is sent back to Junos Space. Junos Space looks up the remote profile based on this remote profile name and determines the set of functions that the user is allowed to perform.

Even in the case of remote-only mode, you might want to create local user accounts in Junos Space in either of the following cases:

- You want to ensure that a user is allowed to log in to Junos Space even if all the AAA servers are down. In this case, if a local user account exists in the Junos Space database, the user session is authenticated and authorized based on the local data. You might choose to do this for a few important user accounts for whom you want to ensure access even in this scenario.
- You want to use device partitions to partition a device into subgroups and assign these subobjects to different users. You use device partitions to share the physical interfaces, logical interfaces, and physical

inventory elements across multiple subdomains. Device partitions are supported only on M Series and MX Series routers. For more information, see the "Creating Device Partitions" on page 422 topic in the *Junos Space Network Management Platform Workspaces User Guide*.

For more information about user authentication, see the "Junos Space Authentication Modes Overview" on page 1458 topic (in the *Junos Space Network Management Platform Workspaces User Guide*).

Certificate–Based and Certificate Parameter–Based Authentication

Junos Space Network Management Platform supports certificate–based and certificate parameter–based authentication for a user. Starting from Release 15.2R1, you can also authenticate users in certificate parameter–based authentication mode. With certificate–based and certificate parameter–based authentication, instead of authenticating a user based on the user's credentials, you can authenticate a user based on the user's certificate and certificate parameters. These authentication modes are considered more secure than password-based authentication. With certificate parameter–based authentication, you can define a maximum of four parameters that are authenticated during the log in process. Certificate–based and certificate parameter–based authentication over an SSL connection can be used to authenticate and authorize sessions among various servers and users. These certificates can be stored on a smart card, a USB drive, or a computer's hard drive. The users typically swipe their smart card to log in to the system without entering their username and password.

For more information about certificate–based and certificate parameter–based authentication, see the "Certificate Management Overview" on page 1426 topic in the Junos Space Network Management Platform Workspaces Feature Guide.

User Roles

When configuring Junos Space, you must decide how you want to segregate users based on the system functionality that users are allowed to access. You do this by assigning a different set of roles to different users. A *role* defines a collection of workspaces that a Junos Space user is allowed to access and a set of actions that the user is allowed to perform within each workspace. To evaluate the predefined user roles that the Junos Space Network Management Platform supports, navigate to the **Roles** page (**Network Management Platform > Role Based Access Control > Roles**). In addition, every Junos Space application that is installed on the Junos Space Network Management Platform has its own predefined user roles. The Roles page lists all existing Junos Space application roles, their descriptions, and the tasks that are included in each role.

If the default user roles do not meet your needs, you can configure custom roles by navigating to the **Create Role** page (**Network Management Platform > Role Based Access Control > Roles > Create Role**).

To create a role, you select the workspaces that a user with this role is allowed to access, and for each workspace, choose the set of tasks that the user can perform from that workspace.

> **NOTE:** You might need to go through several iterations of creating user roles to arrive at the optimal set of user roles that your organization needs.

After the user roles are defined, they can be assigned to various user accounts (in the case of local user accounts created in Junos Space) or assigned to remote profiles to be used for remote authorization.

For more information about configuring user roles, see the "Role-Based Access Control Overview" on page 995 topic (in the *Junos Space Network Management Platform Workspaces User Guide*).

Remote Profiles

Remote profiles are used in the case of remote authorization. A remote profile is a collection of roles defining the set of functions that a user is allowed to perform in Junos Space. There are no remote profiles created by default, and you need to create them by navigating to the **Create Remote Profile** page (**Network Management Platform > Role Based Access Control > Remote Profiles > Create Remote Profile**). When creating a remote profile, you need to select one or more roles that belong to it. Then you can configure the name of the remote profile for one or more user accounts in the remote AAA servers.

When an AAA server successfully authenticates a user session, the AAA server includes the configured remote profile name for that user in the response message that comes back to Junos Space. Junos Space looks up the remote profile based on this name and determines the set of roles for the user. Junos Space then uses this information to control the set of workspaces the user can access and the tasks the user is allowed to perform.

> **NOTE:** If you decide to use local authorization along with remote authentication, you do not need to configure any remote profiles. In this case, you must create local user accounts and assign roles to these user accounts. The configured AAA servers perform authentication, and for each authenticated session, Junos Space performs the authorization based on the roles configured locally for the user account in the database.

For more information about creating remote profiles, see the "Creating a Remote Profile" on page 1098 topic (in the *Junos Space Network Management Platform Workspaces User Guide*).

Domains

You can add, modify, or delete a domain from the **Domains** page (**Role Based Access Control > Domains**). This page is accessible only when you are logged in to the global domain, which means that you can add, modify, or delete a domain only from the global domain. By default, any domain you create is added under the global domain. When you add a domain, you can choose to allow users in this domain to have read-only access to the parent domain. If you choose to do so, then all users in the subdomain can view objects of the parent domain in read-only mode.

> **NOTE:** Only two levels of hierarchy are supported: the global domain and any other domains that you might add under the global domain.

For more information about managing domains, see the "Domains Overview" on page 1077 topic (in the *Junos Space Network Management Platform Workspaces User Guide*).

User Accounts

You need to create user accounts in Junos Space in the following cases:

- To perform local authentication and authorization—You create user accounts in Junos Space. Each user account must contain a valid password and a set of user roles. To create user accounts, navigate to the **Create User** page (**Network Management Platform > Role Based Access Control> User Accounts > Create User**).
- To perform remote authentication and local authorization—You create a user account for each user of the system and ensure that a set of roles is assigned to each user account. It is not mandatory to enter a password for the user accounts because authentication is performed remotely.
- To perform remote authentication and authorization and allow certain users to be able to access Junos Space even if all AAA servers are down or are not reachable from Junos Space—You create local user accounts for these users with a valid password. The system forces you to configure at least one role for these users. However, authorization is performed based on the remote profile name that the AAA server provides.
- To perform remote authentication and authorization but also override remote authentication failures for specified users and allow them to access Junos Space— A typical scenario would be when you need to create a new Junos Space user but do not have immediate access to configure the user on the remote

AAA servers. You must create local user accounts for such users with a valid password and a valid set of roles.

- To perform remote authentication and authorization but also segregate devices among users based on domains—Because domains must be assigned to user objects in Junos Space, you must create remote profiles in Junos Space and assign roles and domains to those profiles.

> **NOTE:** If you decide to use local authorization along with remote authentication, you do not need to configure any remote profiles. In this case, you must create local user accounts and assign roles to these user accounts. The configured AAA servers perform authentication, and for each authenticated session, Junos Space performs the authorization based on the roles configured locally for the user account in the database.

> **NOTE:** Junos Space enforces certain rules for valid passwords. You configure these rules as part of the Network Management Platform settings from the **Applications** page (**Network Management Platform > Administration > Applications**). Right-click the application and select **Modify Application Settings**. Then select **Password** on the left side of the window. On the subsequent page, you can view and modify the current settings.

For more information about creating user accounts, see the "Creating Users in Junos Space Network Management Platform" on page 1035 topic (in the *Junos Space Network Management Platform Workspaces User Guide*).

Device Partitions

You can partition a device from the **Devices** page (**Network Management Platform > Devices > Device Management**). You can partition a device into subgroups and then assign these subobjects to different users by assigning the partitions to different domains. Only one partition of a device can be assigned to a domain.

> **NOTE:** Device partitions are supported only on M Series and MX Series routers.

For more information about device partitions, see the "Creating Device Partitions" on page 422 topic (in the *Junos Space Network Management Platform Workspaces User Guide*).

Release History Table

Release	Description
15.2R1	Starting from Release 15.2R1, you can also authenticate users in certificate parameter–based authentication mode.

RELATED DOCUMENTATION

Installing and Upgrading Junos Space Software Overview | 61

Backing Up the Junos Space Platform Database | 68

3

CHAPTER

Junos Space Network Management

Device Management in Junos Space Platform | 79

Device Configuration Management in Junos Space Platform | 83

Device Management in Junos Space Platform

IN THIS SECTION

- Discovering Devices | 80
- Authenticating Devices | 81
- Viewing the Device Inventory | 82
- Upgrading Device Images | 82

When using Junos Space to manage your network, you must first discover the devices in your network through a device discovery profile, add these devices to the Junos Space Platform database, and allow the devices to be managed by Junos Space Platform. When devices are successfully discovered and managed by Junos Space Platform, the following actions occur:

- A dedicated Device Management Interface (DMI) session is established between Junos Space and each device. This DMI session typically rides on top of an SSHv2 connection with the device. For devices running the export version of Junos OS (ww Junos OS devices), DMI uses a Telnet connection through the wwadapter. The DMI session is maintained till the device is deleted from Junos Space, which means that the session is reestablished in case of transient network problems, device reboots, Junos Space restarts, and so forth.
- When the network itself is the system of record (NSOR), Junos Space imports the complete configuration and inventory of the device into its own database. To keep device information current, Junos Space listens to system log events raised by the device that indicate device configuration or inventory changes, and Junos Space automatically resynchronizes its database with the latest information from the device. When the Junos Space Network Management Platform is the system of record (SSOR), Junos Space reflects the changes on the device, but a Junos Space user with appropriate user privileges must resolve out-of-band changes.
- By default, Junos Space adds itself as an SNMP trap destination by automatically inserting the appropriate SNMP configuration on the device during device discovery; however, you can disable this behavior from the **Network Management Platform > Administration > Applications Network Management Platform > Modify Application Settings** page.
- Junos Space uses SNMP polling to collect key performance indicators (KPIs) from the devices. To enable SNMP polling on managed devices requires that the Network Monitoring feature be turned on.

  NOTE: By default, Junos Space Network Monitoring is turned on for all devices.

NOTE: Starting from Release 16.1R1, you can use a NAT server to discover and manage devices that are outside your Junos Space network and which cannot reach Junos Space Platform. When you add a NAT configuration on the **Administration > Fabric > NAT Configuration** page and forwarding rules on the NAT server, the IP addresses translated through the NAT server are added to the outbound ssh stanza of the external devices.

The following sections list the device management capabilities of Junos Space Platform:

Discovering Devices

Before you can discover devices into Junos Space, ensure the following:

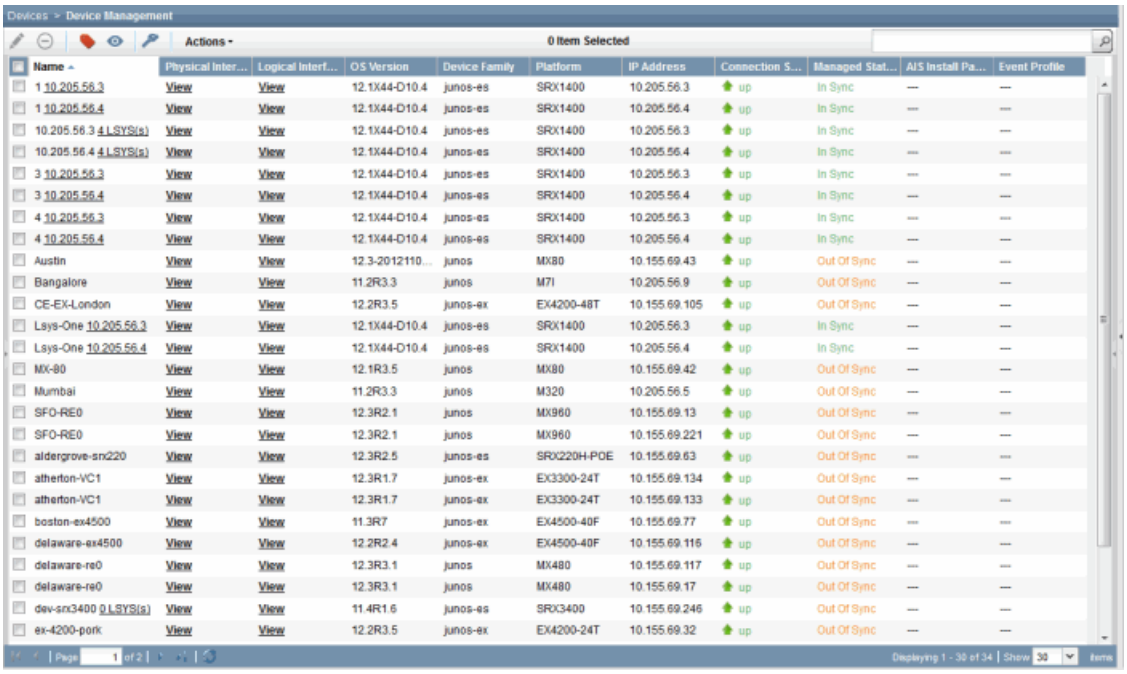
- You know the key details about the devices to discover. You provide this information as input to discover devices:
  - Device details–IP address or hostname of the device or subnet to scan
  - Credentials–User ID and password of a user account that has appropriate user privileges on the device
  - SNMP Credentials–Community string with read-only access if you are using SNMPv2c or valid SNMPv3 credentials. SNMP credentials are not required if you do not plan to use Junos Space to monitor faults and performance of managed devices.
- The IP address of the device can be reached from your Junos Space server.
- SSHv2 is enabled on the device (**set system services ssh protocol protocol-version v2**) and any firewalls along the way allow Junos Space to connect to the SSH port (default TCP/22) on the device. To discover devices running the export version of Junos OS, the wwadapter must be installed on Junos Space and Telnet must be enabled on the device and reachable from Junos Space.
- SNMP port (UDP/161) on the device is accessible from Junos Space, which allows Junos Space to perform SNMP polling on the device to collect KPI data for performance monitoring.
- SNMP trap port (UDP/162) on Junos Space is accessible from the device, which allows the device to send SNMP traps to Junos Space for fault management.

Starting from Release 16.1R1, you can create a device discovery profile (in the Devices workspace) to set preferences for discovering devices. After verifying the prerequisites, you create a device discovery profile from the **Network Management Platform > Devices > Device Discovery Profiles** page. The device discovery profile contains the preferences to discover devices, such as, device targets, probes, authentication details, SSH credentials, and a schedule at which the profile should be run to discover devices. You can also manually run the device discovery profile from the **Network Management Platform > Devices > Device Discovery Profiles** page. The time required to complete the discovery process depends on multiple factors

such as the number of devices you are discovering, the size of configuration and inventory data on the devices, the network bandwidth available between Junos Space and the devices, and so forth.

After your devices are successfully discovered in Junos Space, you can view the devices from the **Network Management Platform > Devices > Device Management** page. The Connection Status for the discovered devices should display “Up” and the managed status should be “In Sync” as shown in Figure 4, which indicates that the DMI session between Junos Space and the device is up and that the configuration and inventory data in Junos Space is in sync with the data on the device.

Figure 4: Device Management Page



For complete information about discovering and managing devices, see the Devices workspace documentation in the *Junos Space Network Management Platform Workspaces User Guide*.

Authenticating Devices

Starting from Release 16.1R1, new enhancements to device authentication are introduced. Junos Space Network Management Platform can authenticate a device by using credentials (username and password), 2048 bit or 4096 bit keys (which uses public-key cryptographic principles such as RSA, DSS, ECDSA), or the device’s SSH fingerprint. You can choose an authentication mode on the basis of the level of security needed for the managed device. The authentication mode is displayed in the Authentication Status column on the Device Management page. You can also change the authentication mode. You need to ensure the following to use these modes of authentication:

- Credentials-Based–Device login credentials with administrative privileges are configured on the device before the device connects to Junos Space Platform.
- Key-Based (keys generated by Junos Space Platform)–By default, a Junos Space installation includes an initial public and private key pair. You can generate a new key pair from the Administration workspace and upload the Junos Space's public key to the devices that are to be discovered from the Devices workspace. Junos Space logs in to these devices through SSH and configures the public key on all the devices. You need not specify a password during device discovery; you need to specify only the username.
- Custom key-based–A private key and an optional passphrase. You can upload the private key to Junos Space Platform and use the passphrase to authenticate the private key. You don't need to upload the private key to devices.

For complete information about device authentication, see the Devices workspace documentation in the *Junos Space Network Management Platform Workspaces User Guide*.

Viewing the Device Inventory

Junos Space Platform maintains up-to-date inventory details of all managed devices in the database. This includes the complete hardware, software, and license inventory of each device as well as details of all physical and logical interfaces on these devices. You can resynchronize a managed device with the Junos Space Platform database to fetch the current configuration and inventory details.

You can view and export hardware, software, and license inventory details, and the physical and logical interfaces of a device from the Junos Space user interface. You can acknowledge the inventory changes on a device from the Junos Space user interface. For complete information about these tasks, see the Devices workspace documentation in the *Junos Space Network Management Platform Workspaces User Guide*.

Upgrading Device Images

Junos Space Platform can be a central repository for all device OS images and provide workflows to download and install these images on managed devices. You can upload, stage, and verify the checksum of device images, and deploy device images and Junos Continuity software packages to a device or multiple devices of the same device family simultaneously from the Images and Scripts workspace. For complete information about upgrading device images, see the Images and Scripts workspace documentation in the *Junos Space Network Management Platform Workspaces User Guide*.

Release History Table

Release	Description
16.1R1	Starting from Release 16.1R1, you can use a NAT server to discover and manage devices that are outside your Junos Space network and which cannot reach Junos Space Platform.
16.1R1	Starting from Release 16.1R1, you can create a device discovery profile (in the Devices workspace) to set preferences for discovering devices.
16.1R1	Starting from Release 16.1R1, new enhancements to device authentication are introduced.

RELATED DOCUMENTATION

DMI Schema Overview | 67

Device Configuration Management in Junos Space Platform

IN THIS SECTION

- Modifying the Device Configuration by Using the Schema-Based Configuration Editor | 84
- Modifying the Device Configuration by Using Device Templates | 85
- Viewing Configuration Changes | 85
- Backing Up and Restoring Device Configuration Files | 86

Junos Space Platform maintains an up-to-date database copy of the complete configuration of each managed device. You can view and modify the device configurations from the Junos Space user interface. Because a Junos device configuration is described in terms of an XML schema and Junos Space Platform has access to this schema, Junos Space user interface uses this schema to graphically render the device configuration. With an up-to-date schema, you can view and configure all configuration options as you would modify the configuration from the device CLI.

By default, Junos Space Platform operates in the mode where it considers the network as the system of record (NSOR). In this mode, Junos Space Platform listens to all configuration changes on managed devices and automatically resynchronizes its database copy with the modified device configuration to reflect the changes. You can change this to a mode where Junos Space considers itself as the system of record (SSOR). In this mode, Junos Space Platform does not automatically synchronize its copy of the device configuration with the modified device configuration when it receives information about out-of-band configuration changes made on a managed device. Instead, the device is marked as *Device Changed* and you can view the changes and decide whether to accept the changes. If you accept the changes, the changes are written into the Junos Space Platform database copy of the device configuration. If you reject the changes, Junos Space Platform removes the configuration from the device. For complete information about NSOR and SSOR modes, see the Devices workspace documentation in the *Junos Space Network Management Platform Workspaces User Guide*.

The following sections list the device configuration management capabilities of Junos Space Platform:

Modifying the Device Configuration by Using the Schema-Based Configuration Editor

You modify the configuration on a single device by using the Schema-based Configuration Editor. To modify a device configuration on a device, right-click the device listed on the Device Management page (in the Devices workspace) and select **Modify Configuration**. You can view the following details:

- Current configuration on the device
- Tree view of the device's configuration hierarchy. Click and expand this tree to locate the configuration stanzas of interest. For more information about the configuration options on a device, refer to Junos OS technical documentation.
- Options to filter the configuration and search for specific configuration options in the tree
- Details of a configuration node when you click the node in the tree
- Options to create, edit, delete, and order entries on the list when you navigate within a configuration node

- Options to view information about individual parameters (blue information icons), add comments about individual parameters (yellow comment icons), and activate or deactivate a configuration option
- Options to preview, validate, and deploy the configuration to the device

For complete information about modifying and deploying the configuration by using the Schema-based Configuration Editor, see the Devices workspace documentation in the *Junos Space Network Management Platform Workspaces User Guide*.

Modifying the Device Configuration by Using Device Templates

You may need to create a common configuration change and push it to multiple devices. You can use the Device Templates feature in Junos Space Platform to create and deploy changes from the Junos Space user interface. You first create a template definition to restrict the scope of a device template to a specific device family and Junos OS version. You then create a device template by using the template definition. You can also create and deploy a configuration by using Quick templates (without using a template definition). You can validate the templates, view the configuration in multiple formats, and deploy (or schedule the deployment of) the configuration to multiple devices. For complete information about creating and deploying a configuration to devices by using device templates, see the Device Templates workspace documentation in the *Junos Space Network Management Platform Workspaces User Guide*.

Viewing Configuration Changes

Junos Space Platform tracks all the configuration changes (from the Schema-Based Configuration Editor, Device Templates feature, Junos Space applications, or the device CLI) made on managed devices. You can view the list of configuration changes on the device in multiple formats from the Junos Space user interface. To view the list of configuration changes, right-click the device and select **View Configuration Change Log**. Each configuration change log entry includes details such as the timestamp of change, user who made the change, the configuration change in XML format, whether the change was made from Junos Space or out-of-band, and also the name of the application or feature that was used to change the configuration. If you have set up Junos Space Platform as the system of record, out-of-band configuration changes on a device modify the managed status of the device to *Device Changed*. You can view and resolve such out-of-band changes by selecting the device and selecting Resolve Out-of-band Changes. You can view a list of all out-of-band changes made on the device. You can accept or reject the changes.

For complete information about viewing configuration changes, see the Device Templates workspace documentation in the *Junos Space Network Management Platform Workspaces User Guide*.

Backing Up and Restoring Device Configuration Files

Junos Space Platform allows you to maintain multiple versions of device configuration files (running, candidate, and backup configuration of managed devices) in the Junos Space Platform database. You can recover device configuration files in case of a system failure and maintain consistent configuration across multiple devices. You can select and back up the configuration from multiple devices from the Configuration Files workspace. A separate configuration file is created in the database for each managed device. For complete information about backing up and restoring device configuration files, see the Configuration Files workspace documentation in the *Junos Space Network Management Platform Workspaces User Guide*.

RELATED DOCUMENTATION

DMI Schema Overview | 67

User Interface Guide

4

CHAPTER

Overview

Junos Space User Interface Overview | 89

Junos Space Home Page Overview | 94

Junos Space User Interface Overview

IN THIS SECTION

- Junos Space Banner | 90
- Task Tree | 91
- Main Window | 93

The Junos Space UI is designed to look and behave in a way that most users are familiar with. The left tree structure facilitates navigation and the right pane displays information about the workspace or task selected in the left pane. Multiple users can access the UI through Web browsers concurrently. All users have access to the same current information in the same system wide database. Access to tasks and objects is controlled by permissions assigned to each user.

The Junos Space UI is common to Junos Space Network Management Platform and Junos Space applications. The information displayed on the Junos Space UI changes according to the application you select. The examples shown here are from the Junos Space Platform UI. Other applications may have design variations.

When you log in to Junos Space Platform, the previously configured home page is displayed. The Junos Space Platform Dashboard, which is the default home page, is shown in Figure 5.

Figure 5: Junos Space Platform Default Home Page

1–Junos Space Banner	4–Global Action Icons
2–Global Search Text Box	5–Junos Space Dashboard
3–Domain Switcher	6–Task Tree

This display contains three main parts: a task tree on the left, which is always available; a main window on the right, whose content changes as you select items from the task tree; and a banner across the top, which offers the date and time, the domain to which you are logged in, global search, and several icon buttons for frequently used actions. These parts are described in the following sections.

Junos Space Banner

The Junos Space banner, as indicated in Figure 5, displays the date and server time in the active time zone, the domain to which you are logged in, global search, and the global actions icons. This banner is always present. For more information about global search and domain features, see "Using Global Search" on page 173 and the "Domains Overview" on page 1077 topic (in the *Junos Space Network Management Platform Workspaces User Guide*).

> **NOTE:** If you access the Junos Space Platform UI in two tabs of the same browser with two different domains selected and access the same page in both tabs, the information displayed on the page is based on the latest domain selected. To view pages that are accessible only in the Global domain, ensure that you are in the Global domain in the most recent tab in which you are accessing the UI.

Table 4 describes the global action icons on the right side of the banner.

Table 4: Global Action Icons

Global Action Icon	Description
	Enables you to access the Junos Space home page or set the Junos Space home page. Refer to the "Setting and Accessing the Junos Space Home Page" on page 102 for details.
	Displays the application Help. To access workspace context-sensitive Help, click the Help icon after navigating to that workspace. See "Accessing Help on Junos Space" on page 106.
	Displays the My Jobs dialog box from which you can view the progress and status of your current managed jobs. You can view all your completed, in-progress, canceled, and scheduled jobs in Junos Space Platform. See "Viewing Your Jobs" on page 175 in the *Junos Space Network Management Platform Workspaces User Guide*.
	Displays the Change User Settings dialog box from which you can change user preferences, such as the password. See "Changing Your Password on Junos Space" on page 177.
	Logs you out of the system. See "Logging Out of Junos Space" on page 178.

Task Tree

The task tree on the left side of the display is always present and facilitates navigation in the Junos Space Platform UI. As shown in Figure 5, when you first log in, the Application Selector list displays Network Management Platform by default. You can drop this list down to see all the Junos Space applications available on your system. (You can install other applications by using the Applications task group, as described in "Managing Junos Space Applications Overview" on page 1328 in the *Junos Space Network Management Platform Workspaces User Guide*.)

You can collapse the task tree to the left by clicking the double left arrow buttons in its header, and reexpand it by clicking the double right arrow buttons.

Below the application name is the word **Dashboard**, selected by default. It indicates that what you see in the right-hand window is the dashboard for the current application—in this case, Junos Space Platform. The dashboard shows several measures of overall system health.

Below the Dashboard item in the tree is a list of the workspaces available in the current application. This list forms the top level of the task tree. If you select a different application from the **Applications** list, you see the workspace list change. This topic describes the workspaces for Junos Space Platform; for the workspaces in other applications, see the documentation for those applications.

The workspaces in the Junos Space Platform are described at a high level in Table 5.

Table 5: Workspace Names

Workspace Name	Function
Devices	Manage devices, including adding, discovering, importing, and updating them. See "Device Management Overview" on page 189 (in the *Junos Space Network Management Platform Workspaces User Guide*).
Device Templates	Create configuration definitions and templates used to deploy configuration changes on multiple Juniper Networks devices. See "Device Templates Overview" on page 462 (in the *Junos Space Network Management Platform Workspaces User Guide*).
CLI Configlets	Easily apply a configuration to a device. Configlets are configuration tools provided by Junos OS. See "CLI Configlets Overview" on page 534 (in the *Junos Space Network Management Platform Workspaces User Guide*).
Images and Scripts	Deploy, verify, enable, disable, remove, and execute scripts deployed to devices. See "Scripts Overview" on page 673 (in the *Junos Space Network Management Platform Workspaces User Guide*). Download a device image from the Juniper Networks Software download site to your local file system, upload it into Junos Space, and deploy it on one or more devices simultaneously. See "Device Images Overview" on page 613 (in the *Junos Space Network Management Platform Workspaces User Guide*).
Reports	Generate customized reports for managing network resources. See "Reports Overview" on page 768 (in the *Junos Space Network Management Platform Workspaces User Guide*).
Network Monitoring	Assess the performance of your network, not only at a point in time, but also over a period of time. See "Network Monitoring Workspace Overview" on page 799 (in the *Junos Space Network Management Platform Workspaces User Guide*).
Configuration Files	See "Managing Configuration Files Overview" on page 938 (in the *Junos Space Network Management Platform Workspaces User Guide*).

Table 5: Workspace Names *(continued)*

Workspace Name	Function
Jobs	Monitor the progress of ongoing jobs. See "Jobs Overview" on page 965 (in the *Junos Space Network Management Platform Workspaces User Guide*).
Role Based Access Control	Add, manage, and delete users, custom roles, domains, and remote profiles. From this workspace, you can also manage user sessions. See "Configuring Users to Manage Objects in Junos Space Overview" on page 1033 (in the *Junos Space Network Management Platform Workspaces User Guide*).
Audit Logs	View and filter system audit logs, including those for user login and logout, tracking device-management tasks, and displaying services that were provisioned on devices. See "Junos Space Audit Logs Overview" on page 1115 (in the *Junos Space Network Management Platform Workspaces User Guide*).
Administration	Add network nodes, back up your database, manage licenses and applications, or troubleshoot. See "Junos Space Administrators Overview" on page 1136, "Maintenance Mode Overview" on page 1153, and other topics related to the Administration workspace in the (in the *Junos Space Network Management Platform Workspaces User Guide*).

You can expand any of these workspaces by clicking the expansion symbol (+) to the left of its name. When you do so, the next level of the task tree for that workspace opens. Some items at this second level may also be expandable subgroups.

You can expand as many workspaces or task groups as you like; previously expanded ones remain open until you collapse them. The design of the task tree enables you to jump from area to area within an application with the minimum number of selections.

Main Window

When you log in to Junos Space Platform, the main window shows the application dashboard by default. If you have set another home page, the main window displays that page. See "Setting and Accessing the Junos Space Home Page" on page 102 for more information.

When you select a workspace name (as opposed to expanding it), the main window changes and displays graphical statistics for that workspace. This display is called Workspace Statistics. It is similar in functionality to the overall system dashboard, but it pertains only to that workspace. See "Workspace Statistics Page Overview" on page 128 for more information.

Selecting the name of a task group or task within the workspace causes the main window to display an inventory of the objects managed in tabular format. See "Inventory Landing Page Overview" on page 129 for more information.

RELATED DOCUMENTATION

Inventory Landing Page Overview | 129
Workspace Statistics Page Overview | 128
Viewing the Junos Space Platform Dashboard | 126
Using the Getting Started Assistants on Junos Space | 104
Junos Space Home Page Overview | 94

Junos Space Home Page Overview

When you log in to Junos Space Network Management Platform, the default page displayed is the Junos Space Dashboard page. However, you can set a different page as the home page and on subsequent logins to Junos Space Platform, the configured home page is displayed. This is useful because you can configure the home page to the page that you visit frequently or the page that is related to your role; for example, a device administrator might configure the Devices Dashboard page as the home page.

Table 6 displays the list of pages in Junos Space Network Management Platform that you are allowed to set as the home page.

Table 6: Junos Space Platform Pages that Can Be Set as the Home Page

Workspace	Page
None	Junos Space Dashboard

Devices	• (Devices) Dashboard
	• Device Management
	• Device Discovery (Dashboard)
	  ◦ Device Discovery Profiles
	• Unmanaged Devices
	• Model Devices
	  ◦ Connection Profiles
	• Secure Console
	• Device Adapter

Table 6: Junos Space Platform Pages that Can Be Set as the Home Page *(continued)*

Workspace	Page
Device Templates	• (Device Templates) Dashboard • Definitions • Templates
CLI Configlets	• (CLI Configlets) Dashboard • Configlets • Configuration View • Configuration Filter • Xpath and Regex
Images and Scripts	• (Images and Scripts) Dashboard • Images • Scripts • Operations • Script Bundles
Reports	• (Reports) Dashboard • Report Definitions • Generated Reports

Network Monitoring	• (Networking Monitoring) Dashboard
	• Node List
	  ◦ Resync Nodes
	• Search
	• Outages
	• Dashboard
	• Events
	• Alarms
	• Notifications
	• Assets
	• Reports
	• Charts
	• Topology
	• Admin
	  ◦ SNMPv3 Trap Configuration

Configuration Files	• (Configuration Files) Dashboard • Config Files Management

Table 6: Junos Space Platform Pages that Can Be Set as the Home Page *(continued)*

Workspace	Page
Jobs	• (Jobs) Dashboard • Job Management
Role Based Access Control	• (Role Based Access Control) Dashboard • User Accounts • Roles • Domains • Remote Profiles • API Access Profiles • User Sessions
Audit Logs	• (Audit Logs) Dashboard • Audit Log

Administration	• (Administration) Dashboard
	• Fabric
	  ◦ Space Node Settings
	  ◦ SNMP Manager
	  ◦ NAT Configuration
	• Database Backup and Restore
	• Licenses
	• Applications
	• Space Troubleshooting
	  ◦ Log Configuration
	• Platform Certificate
	• CA/CRL Certificates
	• Authentication Servers
	• SMTP Servers
	• Email Listeners
	• Git Repositories
	• Audit Log Forwarding
	• Proxy Server
	• Tags
	• DMI Schemas
	• Hardware Catalog
	• Purging Policy

The Junos Space Platform home page is displayed in the following cases:

- When you log in to Junos Space
- When you the click the **Home** icon on the Junos Space banner and select **Go to homepage**
- When you switch domains and if the page that was displayed prior to the domain switch is not accessible in the new domain

> **NOTE:** If the configured home page is not accessible in the new domain, then the Junos Space Dashboard page is loaded.

> **NOTE:** If an installed Junos Space application supports the Junos Space home page, the Home Page icon is displayed when you access the application; otherwise it is hidden.

For more information about how to set and access the Junos Space home page, refer to "Setting and Accessing the Junos Space Home Page" on page 102.

Release History Table

Release	Description
17.1R1	SNMPv3 Trap Configuration
17.1R1	Hardware Catalog
16.1R2	Space Troubleshooting
16.1R2	Log Configuration
16.1R2	Audit Log Forwarding
15.2R1	Git Repositories

RELATED DOCUMENTATION

Junos Space User Interface Overview | 89

5

CHAPTER

Working in the Junos Space User Interface

Logging In to Junos Space | **100**

Setting and Accessing the Junos Space Home Page | **102**

Using the Getting Started Assistants on Junos Space | **104**

Accessing Help on Junos Space | **106**

Understanding GUI Controls | **106**

Understanding Tooltips and Messages | **118**

Understanding Status Indicators | **123**

Viewing the Junos Space Platform Dashboard | **126**

Workspace Statistics Page Overview | **128**

Inventory Landing Page Overview | **129**

Filter Management in Junos Space Platform User Interface | **137**

Global Search Overview | **164**

Using Global Search | **173**

Viewing Your Jobs | **175**

Changing Your Password on Junos Space | **177**

Logging Out of Junos Space | **178**

Logging In to Junos Space

You can connect to the Junos® Space UI by using your Web browser. The minimum browser requirements supported by Junos Space Network Management Platform are Internet Explorer version 11, Google Chrome version 22, and Mozilla Firefox version 45.

We recommend a screen resolution of 1280 x 1024 pixels or higher.

WARNING: To avoid a Browser Exploit Against SSL/TLS (BEAST) attack, whenever you log in to Junos Space through a browser tab or window, make sure that the tab or window was not previously used to access a non-HTTPS website. Best practice is to close your browser and relaunch it before logging in to Junos Space.

NOTE:

- The Network Monitoring Topology feature of Junos Space Platform is not supported on Internet Explorer.
- Before you log in to Junos Space, ensure that the Adobe Flash version 10 or later plug-in is installed in your browser.

To access and log in to Junos Space:

1. In the address bar of your browser window, enter **https://*virtual-IP-address*/mainui/**, where *virtual-IP-address* is the previously configured virtual IP (VIP) address that is used for Web access to Junos Space.

2. Press Enter or click **Search**.

   The Junos Space login page appears.

3. In the **Username** text box, enter your username. The default username is **super**. For information about how to change your username, consult your system administrator.

4. In the **Password** text box, enter your password. The default password is **juniper123**. For information about how to change your password, see "Changing Your Password on Junos Space" on page 177.

5. (Optional) If the remote authentication server is configured for Challenge/Response, you are presented with challenge questions. Provide valid responses to the challenge questions to log in successfully. For

more information, see “Remote Authentication Overview” on page 1457 in the *Junos Space Network Management Platform Workspaces User Guide*.

6. Click **Log In**.

   The Junos Space home page appears. If the home page is not set, the Junos Space Dashboard page is displayed. If the home page is inaccessible due to role or domain restrictions, a warning message is displayed and the Junos Space Dashboard page is loaded.

   NOTE: If you are a user with access to more than one domain, then an informational message about switching domains is displayed in a dialog box.

   Do one of the following:

   - To prevent the informational message from appearing again, ensure that the **Don’t show again** check box is selected and click **OK**. The **Don’t show again** check box is selected by default.
   - To allow the informational message to continue appearing, clear the **Don’t show again** check box and click **OK**.

NOTE: By default, Junos Space Platform authenticates a user's username and password. However, you can also use certificates to authenticate and authorize sessions among various servers and users. To configure certificate-based authentication, see “Certificate Management Overview” on page 1426 (in the *Junos Space Network Management Platform Workspaces User Guide*).

For more information about the Junos Space Platform UI, see “Junos Space User Interface Overview” on page 89.

RELATED DOCUMENTATION

Logging Out of Junos Space | 178

Setting and Accessing the Junos Space Home Page

IN THIS SECTION

- Setting the Junos Space Home Page | 102
- Accessing the Junos Space Home Page | 104

By default, the Junos Space Network Management Platform Dashboard page is displayed when you log in to Junos Space. You can, however, set a different page as the *home* page. You use the **Home** icon on the Junos Space banner to set and access the Junos Space home page.

> **NOTE:** If you are already on the home page, then the **Set as Homepage'** and **Go to Homepage** actions are disabled. When you mouse over the actions, a message is displayed in a tool tip indicating that you are already on the home page.

This topic has the following sections:

Setting the Junos Space Home Page

To set a page as the home page:

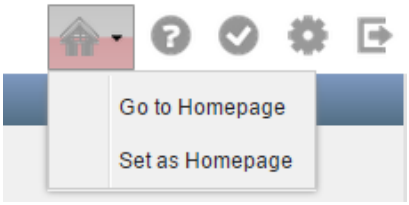
> **NOTE:** For more information about which pages can be set as home pages, see "Junos Space Home Page Overview" on page 94.

1. Navigate to the page that you want to set as the Junos Space home page by using the task tree in the left-hand pane of the Junos Space Platform UI.

2. Click the **Home** icon on the Junos Space banner.

   A drop-down menu is displayed as shown in Figure 6

Figure 6: Home Page Menu



3. Click **Set as Homepage**.

> **NOTE:** The **Set as Homepage** action is enabled or disabled depending on the page that you are on. If the current page can be set as the home page, the action is enabled; otherwise, the action is disabled and when you mouse over the **Set as Homepage** action, a message is displayed (in a tooltip) indicating that the page cannot be set as the home page.

A dialog box is displayed indicating the home page is set successfully.

4. Click **OK** to close the dialog box.

> **NOTE:** When you are not on the home page, click the **Home** icon on the Junos Space banner and mouse over **Go to Homepage** to view the name of the current home page.

Accessing the Junos Space Home Page

To access the Junos Space home page:

> **NOTE:** The roles that you are assigned and the domains to which you have access determine whether or not you can access the home page. If your role does not allow you access to a specific page or if a page is not accessible in a particular domain, a dialog box is displayed when you click the **Go to Homepage** action:
>
> - If the page from which you try to access the home page is the Junos Space Dashboard page, a message indicating that you do not have permission to access the home page is displayed.
> - If the page from which the you try to access the home page is *not* the Junos Space Dashboard page, a message indicating that you do not have permission to access the home page is displayed and you can choose whether to load the Junos Space Dashboard page or remain on the current page.

1. Click the **Home** icon on the Junos Space banner.

   A drop-down menu is displayed as shown in Figure 6

2. Click **Go to Homepage**.

   You are taken to the configured Junos Space home page. On the navigation tree, the node corresponding to the home page is selected and subtasks, if any, are visible.

RELATED DOCUMENTATION

Junos Space User Interface Overview | 89

Using the Getting Started Assistants on Junos Space

The Getting Started assistants display steps and help on how to complete common tasks, such as increasing the storage capacity. Getting Started appears in the sidebar when you log in to Junos Space only if the **Show Getting Started on Startup** check box at the bottom of the sidebar is selected. If the sidebar is not shown, you can display it by selecting the Help icon in the Junos Space banner.

The Getting Started topics are context-sensitive per application. Getting Started displays all the steps of a task. From a step in a task, you can jump to that point in the UI and complete the task.

Some applications implement the Getting Started assistants; others do not.

To use a Getting Started assistant:

1. Select an application from the **Applications** list above the task tree.

2. In the sidebar, expand **Getting Started**.

   A main Getting Started topic link appears on the sidebar.

   If the sidebar is not displayed, select the Help ( ) icon at the right side of the Junos Space header. The sidebar appears.

3. Select a main topic.

   For example, if you are in the Network Management Platform UI, click the **Increase Space Capacity** link. A list of required steps appears in the sidebar. Each step contains a task link and a link to Help.

4. Perform the required task by clicking the task link.

   You move to a point in the UI from where you can complete the task. The assistant remains visible on the sidebar to aid navigation to subsequent tasks.

5. Access help for a specific step by clicking the Help icon next to that step.

To close the Getting Started sidebar, click the double-arrow button on its top-right corner.

RELATED DOCUMENTATION

Accessing Help on Junos Space | 106

Accessing Help on Junos Space

Junos Space provides a Help system that is context-sensitive per workspace. The Help system provides information about each element in the system, including workspaces, dashboards, tasks, inventory pages, and actions. Help topics appear as links on the sidebar.

To access online Help:

1. Click the workspace with which you want to work.
2. Click the Help icon at the right side of the Junos Space header.

   The help icon is represented as .

   The sidebar appears, if it is not already displayed, with the Help section open listing specific topics for that workspace and tasks.
3. Click a topic link to view its contents.

   The Help topic appears in a separate window.
4. Click the icon at the top right of the sidebar to hide it.

For more information about the Junos Space Platform UI, see the "Junos Space User Interface Overview" on page 89 topic.

RELATED DOCUMENTATION

Using the Getting Started Assistants on Junos Space | 104

Understanding GUI Controls

IN THIS SECTION

- Check Box | 107
- Date Picker | 110
- Drop-down List | 111

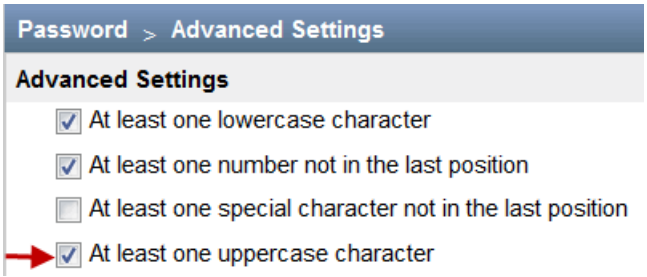
- Option Button | 112
- Search Field | 112
- Spin Box | 113
- Slider | 113
- Text Box | 114
- Tree View | 116
- Scrolling Controls | 117
- Sizing Controls | 118

The following sections describe the various controls that can appear on the Junos Space UI:

Check Box

You can use check boxes to select or deselect an option. For example, to ensure that there is at least one uppercase character when a user creates or modifies a password, an administrator can select the **At least one uppercase character** check box (as shown in Figure 7) on the **Administration** > **Applications** > **Network Management Platform** > **Modify Application Settings** (from the Actions menu) > **Password** > **Advanced Settings** page. On a page, you can select one or more check boxes.

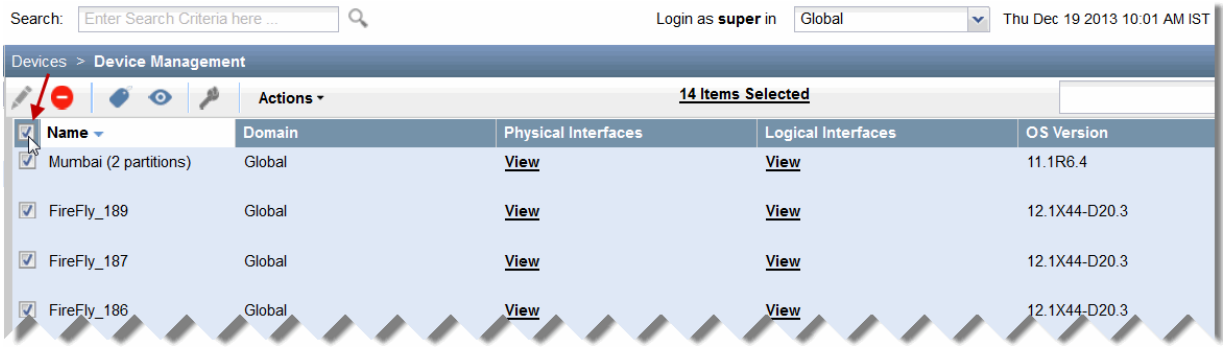
Figure 7: Check Box



Selecting All Objects on a Single Page

With Junos Space, you can select all objects on an inventory landing page by selecting the check box that is displayed adjacent to the first column header. For example, you can select the check box (see Figure 8) adjacent to the **Name** column on the Device Management inventory landing page to select all devices displayed on this page.

Figure 8: Check Box Adjacent to the First Column Header

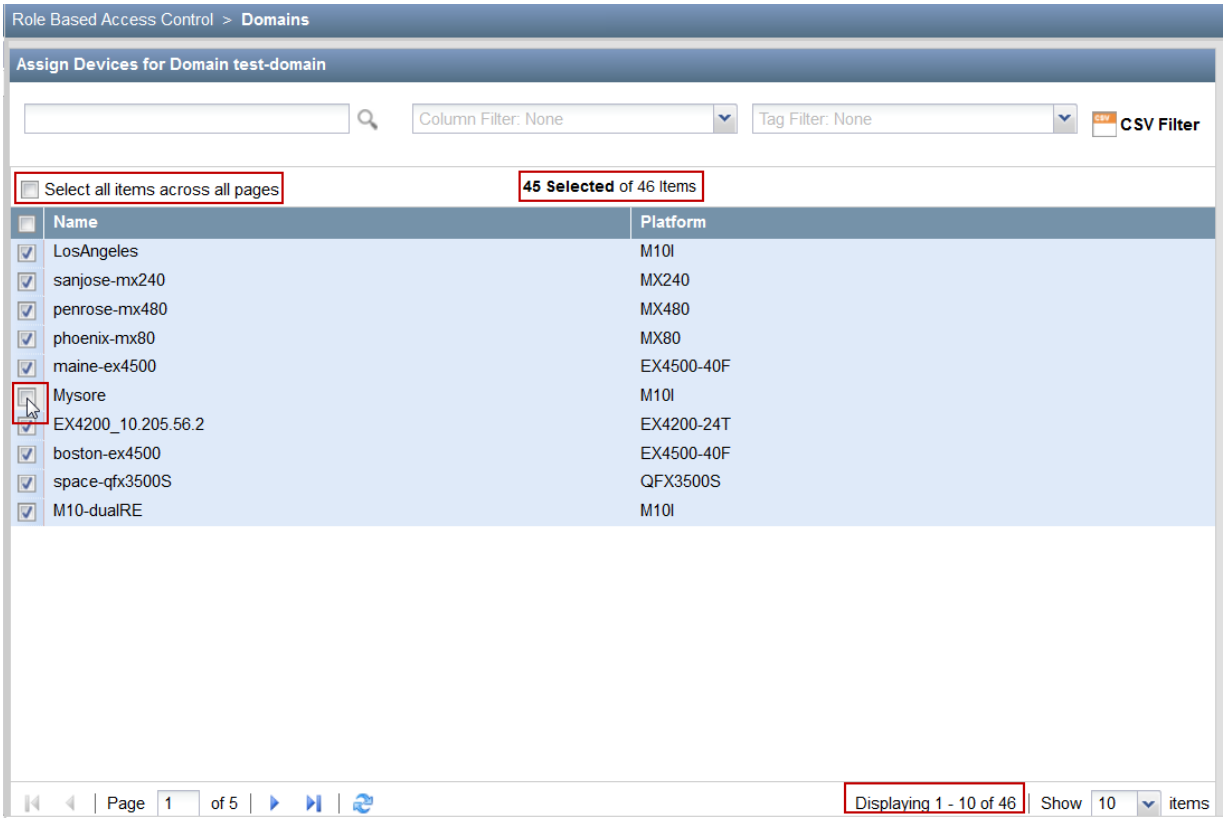


Selecting All Objects Across Multiple Pages

For certain tasks, you can select an appropriate check box in the Junos Space UI to select all objects spread across multiple pages. With this feature, you do not need to select each object individually on multiple pages.

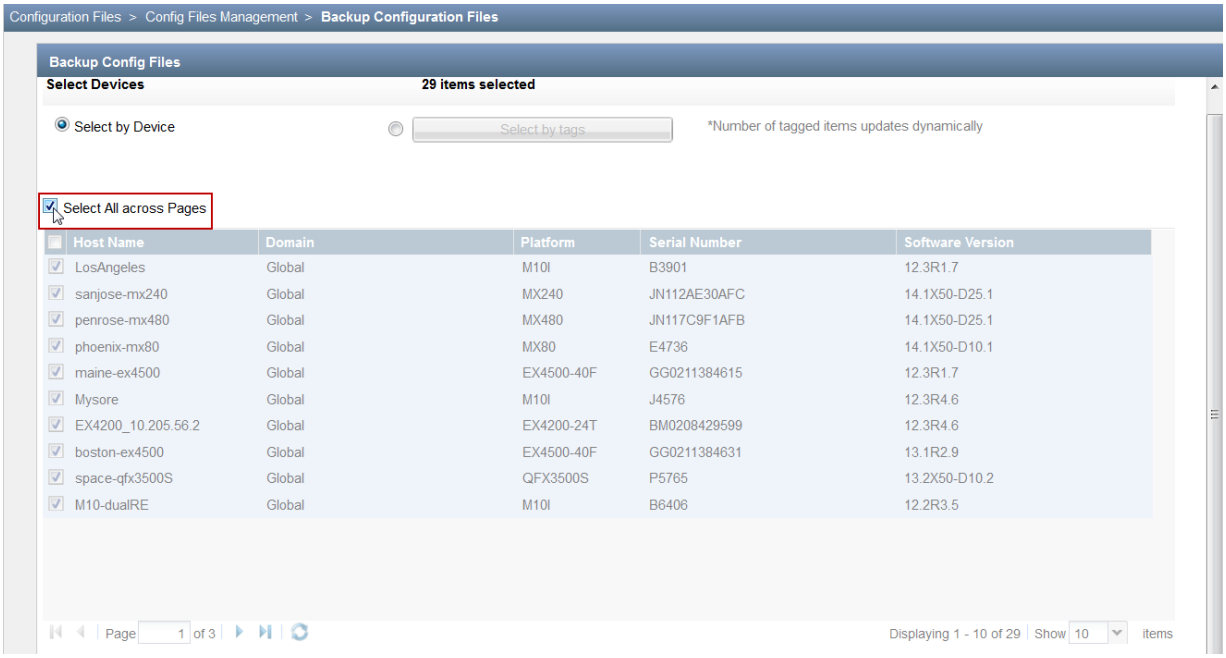
For example, when you want to assign all devices to a domain, you can select the **Select all items across all pages** check box on the Domains page at the time of domain creation, which selects all devices (indicated by the check mark next to the devices as shown in Figure 9). However, after all the devices are selected, you can deselect one or more devices, if needed.

Figure 9: Check Box to Select All Objects Across Multiple Pages: Domains Page



Though some pages support selection of all objects across multiple pages, you may not be able to deselect any of these objects after the selection. For example, when you select the **Select All across Pages** check box when backing up the configuration files (on the **Configuration Files** > **Config Files Management** > **Backup Configuration Files** page), you cannot deselect any of the selected devices (see Figure 10). The configuration of all devices are backed up.

Figure 10: Check Box to Select All Objects Across Multiple Pages: Backup Configuration Files Page



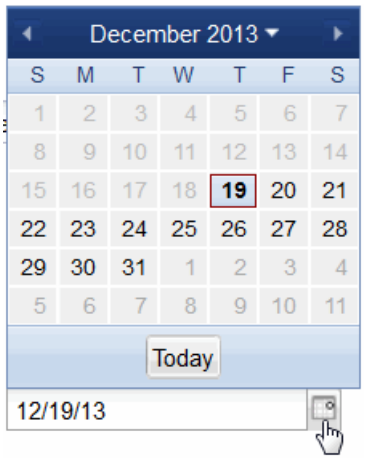
NOTE: Only certain pages in the Junos Space UI support the selection of objects across multiple pages.

Date Picker

Using a date picker, you can select a date by either typing it into a text box or by using a drop-down Calendar control.

In Figure 11, you can specify a date by typing the date in the text box or from the Calendar control by clicking the icon next to the text box. To select today's date, click **Today** on the Calendar control.

Figure 11: Date Picker

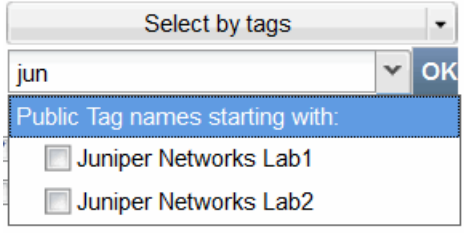


Drop-down List

With a drop-down list, you can select from a list of values (see Figure 12). Clicking the arrow next to the list box opens the list. Junos Space also provides an editable drop-down list, which is a combination of a drop-down list and an editable text box (see Figure 13). You can enter the first few letters in the text box to narrow down the list of values.

Figure 12: Drop-down List

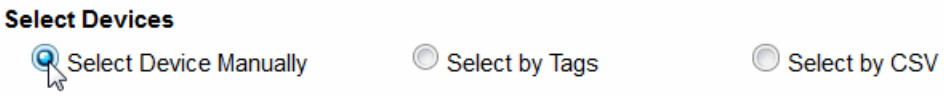
Figure 13: Editable Drop-down List



Option Button

Using an option button, you can make a single choice among a set of mutually exclusive, related options. Only one button at a time can be selected from the available options. The default option is selected (see Figure 14).

Figure 14: Option Button



Search Field

Use the Search text field on the right of the inventory page banner to look for specific objects to display on the inventory landing page. To find objects (within columns) on this page, enter the search criteria in the Search field (see Figure 15). This field supports the same search syntax as the global search field (see "Using Global Search" on page 173). For example, enter "os:junos AND down" to find devices that are down on the Device Management inventory landing page. This feature is more powerful than the column filter because it allows you to use Boolean expressions.

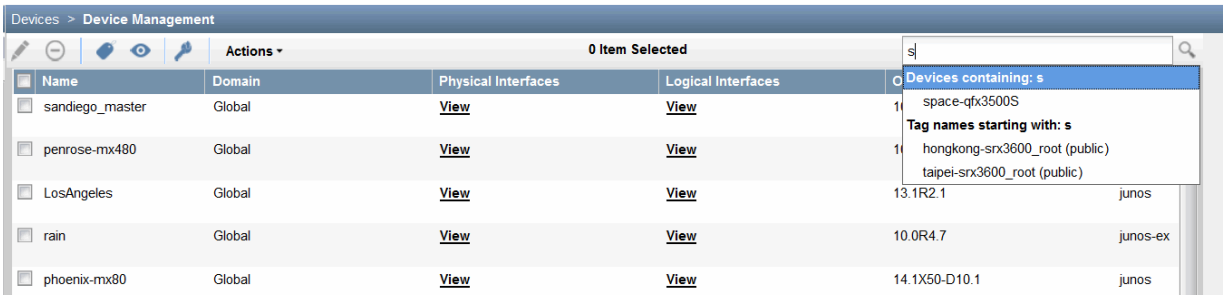
Clicking the magnifying glass at the right of the search field displays a list of objects matching the search criteria. If you press the down arrow after entering the search criteria in the search field , a list of search options is displayed. When you select a search option from the list, only those inventory items that are specific to that search option are displayed on the page.

You can create tags to categorize objects. For more information about tagging objects to select similar objects, see "Tagging an Object" on page 1526 (in the *Junos Space Network Management Platform Workspaces User Guide*).

To display all the inventory objects on the page again, clear the contents of the Search field and press Enter.

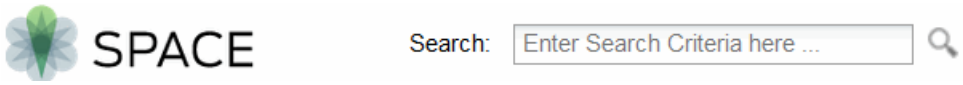
> **NOTE:** You must append "*" if you want to search using partial keywords. Otherwise, the search might return zero matches.

Figure 15: Search Field



To search for specific objects across the entire Junos Space Network Management Platform, use the Search field on the banner at the top of the inventory page (see Figure 16). For more information about global search, see "Using Global Search" on page 173.

Figure 16: Global Search



Spin Box

A spin box is a text box with up and down arrows that you can click to change the value incrementally (see Figure 17). You can also type a valid value in the box.

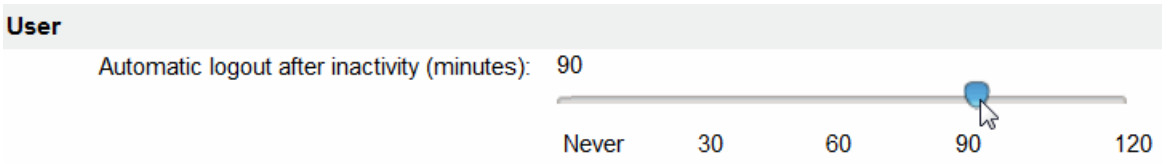
Figure 17: Spin Box

Slider

Using a slider, you can select a value from a continuos range of values by sliding the indicator along a bar. The indicator shows the current value.

In Figure 18, the automatic logout of a user due to inactivity is set to 90 minutes by using the slider control.

Figure 18: Slider



Text Box

A text box enables you to:

- Enter or edit text (for example, the **Login ID** or **Password** fields in Figure 19).
- Upload files from your computer to the Junos Space server, such as the **Image File** or **X509 Cert File** fields in Figure 19.
- Choose a value from a drop-down list of values when you enter the first few letters in the text box (see Figure 20).

Use the label associated with a text box to identify the purpose of a text box. You can gain additional information about some of the text boxes from the information icons that are associated with the text boxes ( ). For example, the **Temporary Password** and **Password** text boxes have information icons associated with them as shown in Figure 19. You must mouse over the information icon for Junos Space to display information about the text box with which the information icon is associated. For example, when you mouse over the information icon associated with the **Password** text box, the conditions that must be met when you enter a password are displayed.

NOTE: Not all text boxes in Junos Space have information icons associated with them.

Figure 19: Text Box

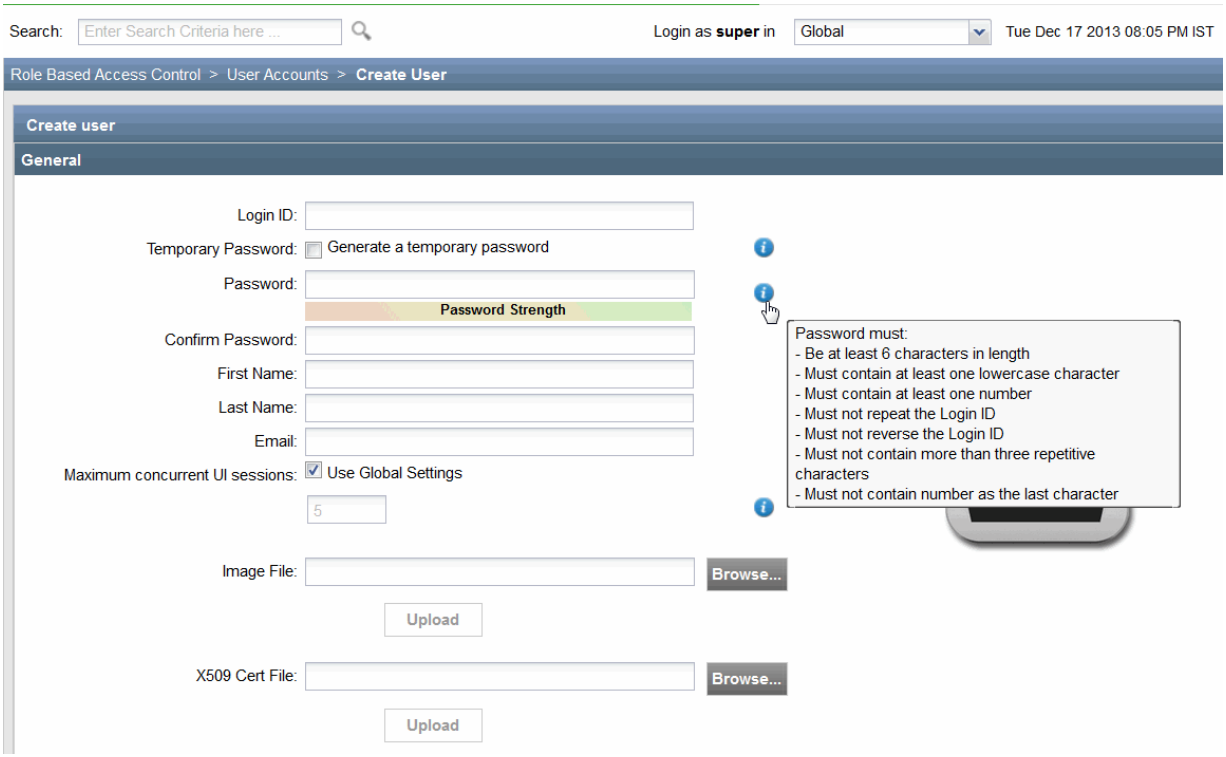
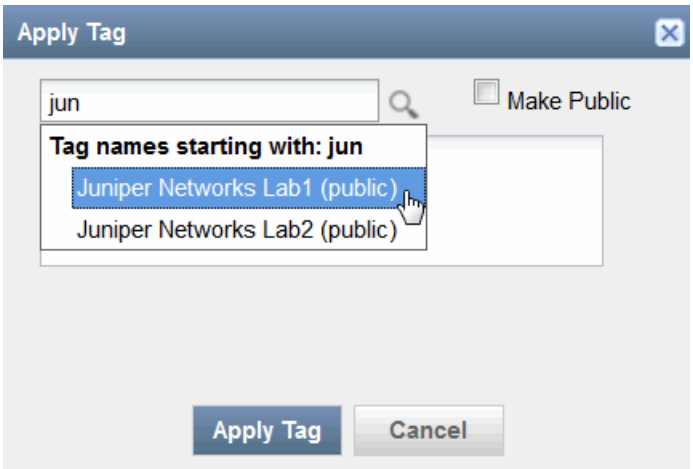


Figure 20: Text Box Displaying a Drop-down List

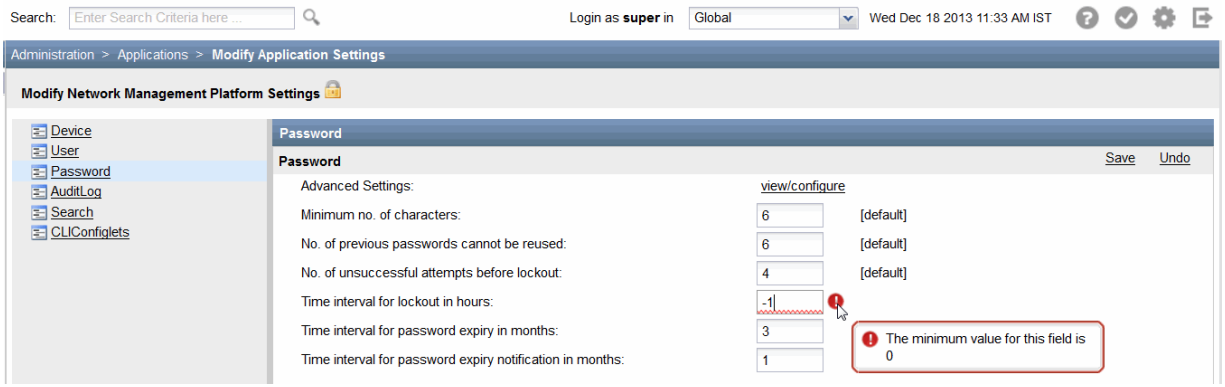


Identifying the Range of Values

Usually, if there is a default value associated with a text box, then it is displayed by default on the text box. However, to determine the range of values that is accepted in a text box, perform the following steps:

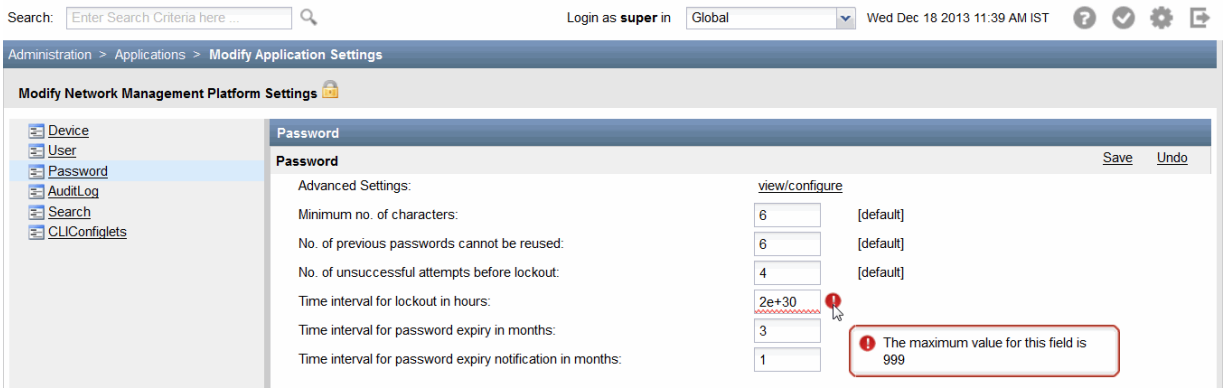
- To determine the minimum value, enter a negative value (for example, –1) in the text box. An error icon appears next to the text box. Mouse over this icon to see the minimum value that is accepted in this text box (see Figure 21).

Figure 21: Minimum Value in a Text Box



- To determine the maximum value, enter a very high value in the text box. An error icon appears next to the text box. Mouse over this icon to see the maximum value that is accepted in this text box (see Figure 22).

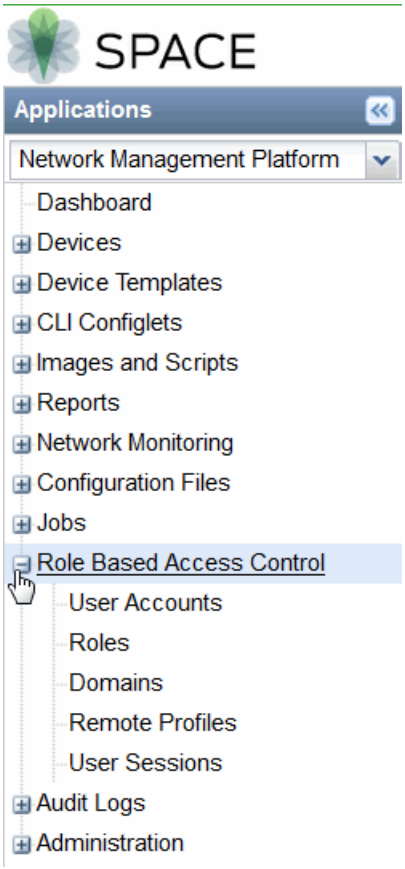
Figure 22: Maximum Value in a Text Box



Tree View

Using the tree view, you can view and interact with a collection of Junos Space objects that are arranged hierarchically. You can select only one object from the objects that are displayed in tree view. You can expand and collapse an object by clicking the plus and minus expander buttons respectively (see Figure 23).

Figure 23: Tree View



Scrolling Controls

Junos Space Network Management Platform provides horizontal and vertical scroll bars on inventory landing pages, which you can use to scroll the contents of the page by clicking one of the scroll arrows, clicking an area in the scroll bar, or dragging the scroll bar. For example, to view data that is at the bottom of the Junos Space page, you can drag the vertical scroll bar toward the bottom of the page. Figure 24 shows the horizontal scroll bar that enables you to scroll horizontally through the Junos Space page allowing you to view data that is on the left or right.

Figure 24: Horizontal Scroll Bar

Sizing Controls

You can use the minimize, maximize, and close buttons of your browser window to hide the Junos Space application window, enlarge the window to fill the whole screen, and close the window, respectively.

> **NOTE:** Minimize the window when you want the Junos Space application window to be temporarily out of the way instead of closing it.
>
> Close the window when you have finished working on it and there is no need for you to return.

To resize a window (make it smaller or bigger), point to any of the window's borders or corners. When the mouse pointer changes to a double-headed arrow, drag the border or corner to shrink or enlarge the window. You cannot resize a window that is already maximized.

Figure 25 displays the minimize, maximize, and close buttons.

Figure 25: Minimize, Maximise, and Close Buttons

RELATED DOCUMENTATION

- Junos Space User Interface Overview | 89

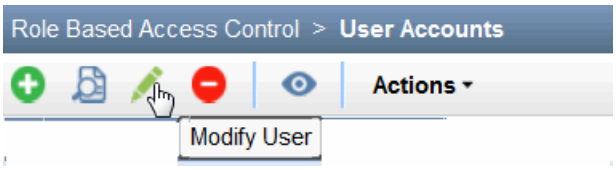
Understanding Tooltips and Messages

IN THIS SECTION

- Error Messages | 119
- Confirmation Messages | 120
- Information Messages | 120
- Standard Icons in Messages | 121

Junos Space Network Management Platform displays tooltips, which are small pop-up windows that provide information about an unlabeled control, such as the information that is displayed automatically when you mouse over an icon on a toolbar (see Figure 26).

Figure 26: Tooltip

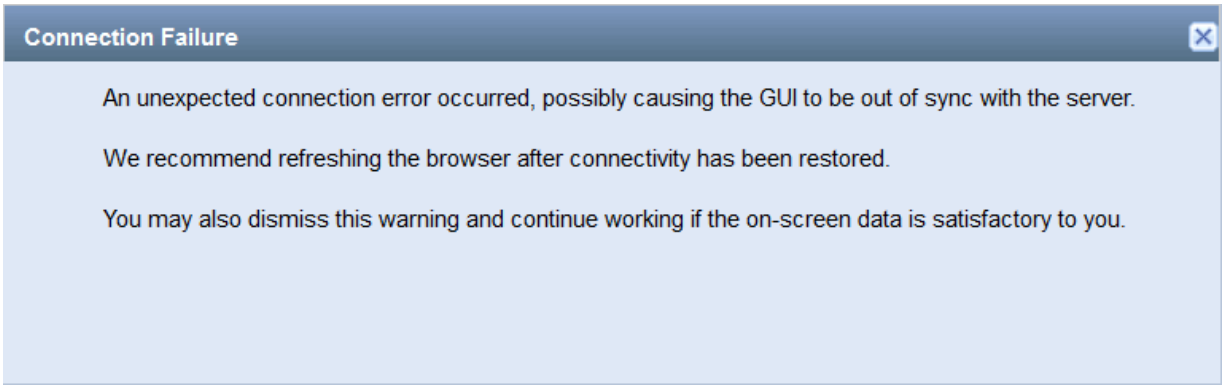


Also, Junos Space sometimes displays pop-up messages to report conditions that require your attention. Depending on the severity level, the icons that are displayed in a message differ. To gain an understanding of the various types of messages and the icons that are displayed in the Junos Space UI, see the following sections:

Error Messages

Junos Space displays an error message to alert you about a problem that has already occurred along with a recommendation, if any, to resolve the problem. For example, in Figure 27, the error message alerts you that the Junos Space UI may be out of sync with the Junos Space server and that you need to refresh the browser window (which is likely to resolve the issue).

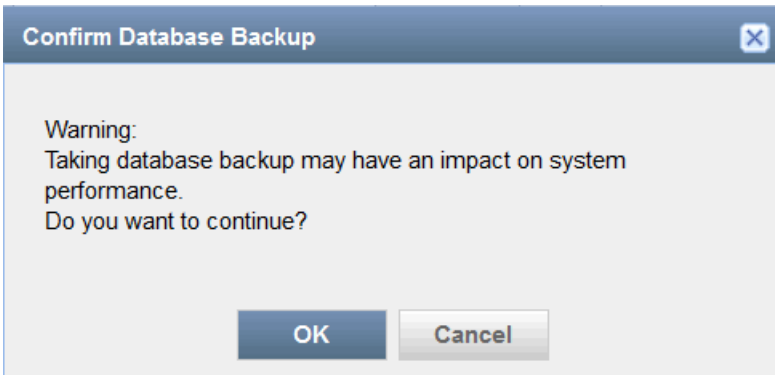
Figure 27: Error Message Dialog Box



Confirmation Messages

Junos Space often displays a confirmation dialog box, which is a modal dialog box that asks you whether you want to proceed with the action that you initiated from Junos Space Network Management Platform. A confirmation dialog box typically consists of a question and two or more responses. You have to select a response and based on your choice Junos Space completes or cancels the task that you initiated. For example, when you initiate a database backup operation, you are asked to confirm whether you want to perform the backup operation because this operation may have an impact on Junos Space performance. In Figure 28, clicking **OK** initiates the database backup operation, whereas clicking **Cancel** closes the current page.

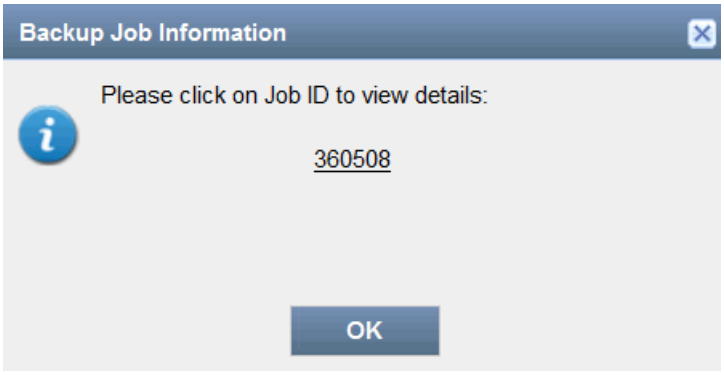
Figure 28: Confirmation Dialog Box



Information Messages

An information message communicates some sort of information to you pertaining to your current activity and appears in a modal dialog box. For example, when you choose to proceed with the database backup operation, Junos Space displays an information message containing a job ID, which you can click to know whether the backup operation is a success or a failure (see Figure 29).

Figure 29: Information Dialog Box



Standard Icons in Messages

Icons that are associated with various messages help you assess the situation at a glance and decide what action to take. If the severity level of the message is high, which is usually indicated by the Error icon, revisit the past action and make suitable corrections (for example, enter missing information in a mandatory field) before you proceed to the next step.

NOTE: Not all messages that are displayed in Junos Space are associated with icons.

Table 7: Standard Junos Space Message Icons

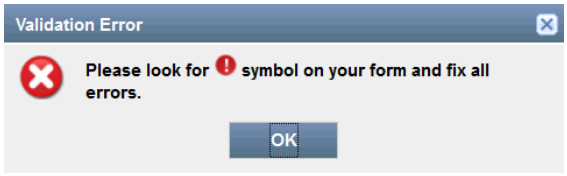
Icon	Description	Message with the Icon
	Error icon—Indicates that an error or problem has occurred, which should be resolved before you proceed	For example, the following error message is displayed if you try to create a tag without a tag name or a user without a username. Providing appropriate information in all fields where the icon appears usually resolves this type of error. Figure 30: Message with the Error Icon 

Table 7: Standard Junos Space Message Icons *(continued)*

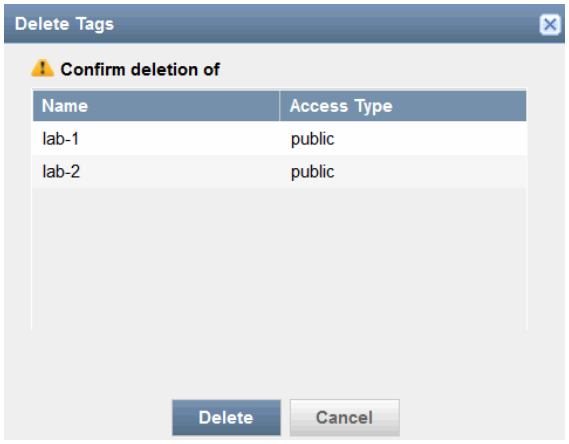
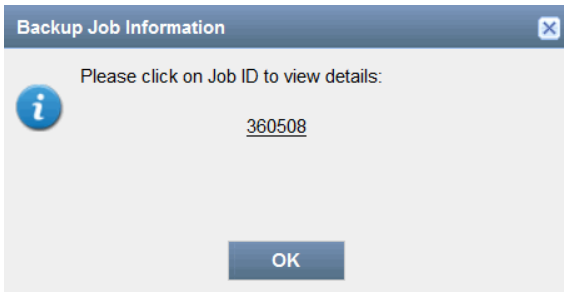
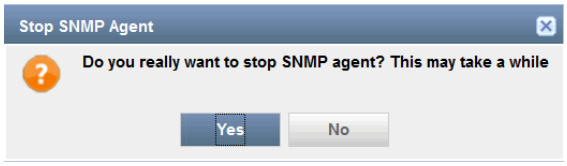
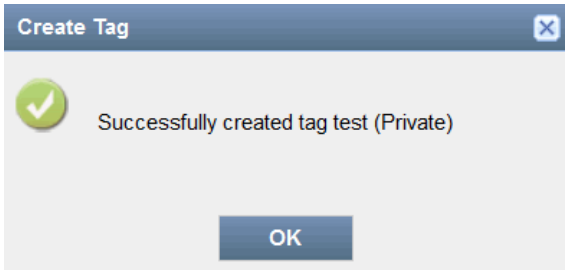
Icon	Description	Message with the Icon
• •	Warning icon—Indicates a condition that might cause a problem in the future These icons come in two different sizes: larger and smaller. A smaller warning icon indicates that you might have to think twice before you proceed with the action. A larger warning icon indicates that the action you initiated cannot be performed because of various constraints.	For example, the following error is displayed when you try to delete an SMTP server that is active: **Figure 31: Message with the Larger Warning Icon** The following message is a warning that you may not be able to retrieve the tags if you confirm the deletion. **Figure 32: Message with the Smaller Warning Icon** 
	Information icon—Presents you with useful information.	The following message indicates that a backup operation is triggered: **Figure 33: Message with the Information Icon** 

Table 7: Standard Junos Space Message Icons *(continued)*

Icon	Description	Message with the Icon
	Question mark icon—Normal confirmation message to which you typically respond with a "Yes" or "No"	Depending on your response to the following message, Junos Space performs a suitable action. **Figure 34: Message with the Question Mark Icon** 
	Check mark icon—Indicates that the action you initiated is a success	The following message indicates that a private tag with the name “test” is successfully created: **Figure 35: Message with the Check Mark Icon** 

RELATED DOCUMENTATION

Junos Space User Interface Overview | 89

Understanding Status Indicators

IN THIS SECTION

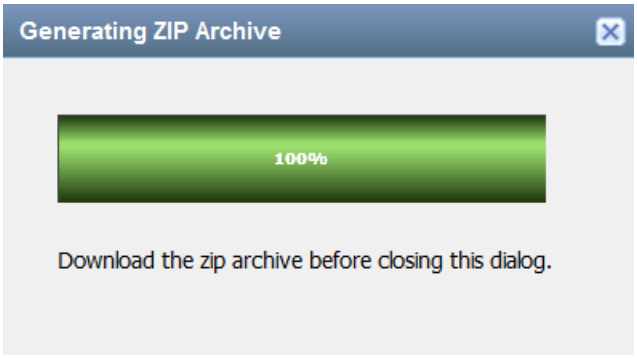
Progress Bars | 124
Status Indicator Icons | 124

Junos Space Network Management Platform status indicators enable you to monitor the status of an action that you initiated from Junos Space. The following status indicators in Junos Space are the most common:

Progress Bars

The progress bar shows you the progress of an action that you initiated from Junos Space. In Junos Space, progress bars are typically displayed when you export files from Junos Space to your computer, add an application to Junos Space, and so on. For example, when you export a configuration file, Junos Space displays the progress of the export action in a dialog box (see Figure 36). When the action is completed, the progress bar displays **100%**.

Figure 36: Progress Bar



Status Indicator Icons

Status indicator icons on an inventory landing page indicate the status of a Junos Space object, such as whether a user is in the enabled or disabled state. Status indicators are not displayed for all Junos Space objects.

Status indicators that are displayed for users are listed in Table 8:

Table 8: User Status Indicators

User Status Indicator	Description
✔	User is in enabled state.

Table 8: User Status Indicators *(continued)*

User Status Indicator	Description
	User is in disabled state. Users in disabled state cannot log in to Junos Space Network Management Platform. For more information about enabling or disabling a user, see "Disabling and Enabling Users" on page 1051 (in the *Junos Space Network Management Platform Workspaces User Guide*).

Status indicators that are displayed for devices are listed in Table 9:

Table 9: Device Status Indicators

Device Status Indicator	Description
	Device is up.
	Device is down. Ensure that the status of the device is up before initiating any action on the device. Actions initiated on devices that are down are likely to fail.
	Device is in synchronized state.

Each job has a job status indicator. Table 10 describes these indicators.

Table 10: Job Icon Status Indicators

Job Status Indicator	Description
	The job was completed successfully.
	The job failed.
	The job was canceled by a user.
	The job is scheduled.
	The job is in progress. You can cancel only those jobs that are in progress from the Actions menu.

RELATED DOCUMENTATION

Junos Space User Interface Overview | 89

Viewing the Junos Space Platform Dashboard

When you log in to Junos Space Network Management Platform, the home page is displayed. By default, the home page for Junos Space Platform is the Dashboard page. However, if you previously configured a different page as the home page, then the configured home page is displayed when you log in.

The Junos Space Platform dashboard, as shown in Figure 37, displays graphs that provide information about the overall system condition, the fabric load history, the active users history, and the percentage of jobs in different states. The charts are visible to all users and are updated in real time.

NOTE: If you do not have user privileges to view detailed data, you might not be able to view detailed information if you select a gadget.

Figure 37: Junos Space Platform Dashboard Page

To access the Junos Space Dashboard page:

1. On the Junos Space Platform UI, select **Dashboard**.

   The Dashboard page is displayed.

2. (Optional) To view more information related to the overall system condition, click **Overall System Condition** or the indicator needle.

You are taken to the Fabric page, where you can view detailed information about the nodes in the fabric. For more information, see "Viewing Nodes in the Fabric" on page 1186.

3. (Optional) To view information related to the fabric load, on the **Fabric Load History** graph:
   - Mouse over a graph data point to view the average CPU usage percentage.
   - Click the blue line depicting the CPU usage to view detailed information.

     You are taken to the Fabric page, where you can view detailed information about the CPU, memory, and disk usage for the nodes in the fabric.
4. (Optional) To view information related to the active users, on the **Active Users History** graph:
   - Mouse over a graph data point to view the total number of active users at that point.
   - Click a data point on the graph to view more information about the active users at that point.

     You are taken to the User Accounts page, where the active users are displayed. For more information, see "Viewing User Statistics" on page 1068.
5. (Optional) To view information related to the jobs, on the **Job Information** graph:
   - Mouse over a segment in the pie chart to view the percentage of jobs with a particular status; for example, cancelled jobs, successful jobs, or failed jobs.
   - Click a segment of the pie chart to view details of jobs with status corresponding to the segment.

     You are taken to the Job Management page, where the jobs filtered by the status are displayed. For more information, see "Viewing Jobs" on page 972.
6. (Optional) You can view records about the health and performance of the Junos Space nodes in your Junos Space setup and the processes on these nodes in a system health report. The health and performance data collected from the nodes is displayed in the System Health Report table. For more information, see "Viewing the Administration Statistics" on page 1138.
7. (Optional) You can move any chart displayed on the Dashboard page by clicking inside the title bar and dragging the chart.
8. (Optional) You can resize any chart displayed on the Dashboard page by hovering over an edge and clicking and dragging the edge.

RELATED DOCUMENTATION

Junos Space Platform Workspaces Overview | **182**

Overall System Condition and Fabric Load History Overview | **1159**

Workspace Statistics Page Overview

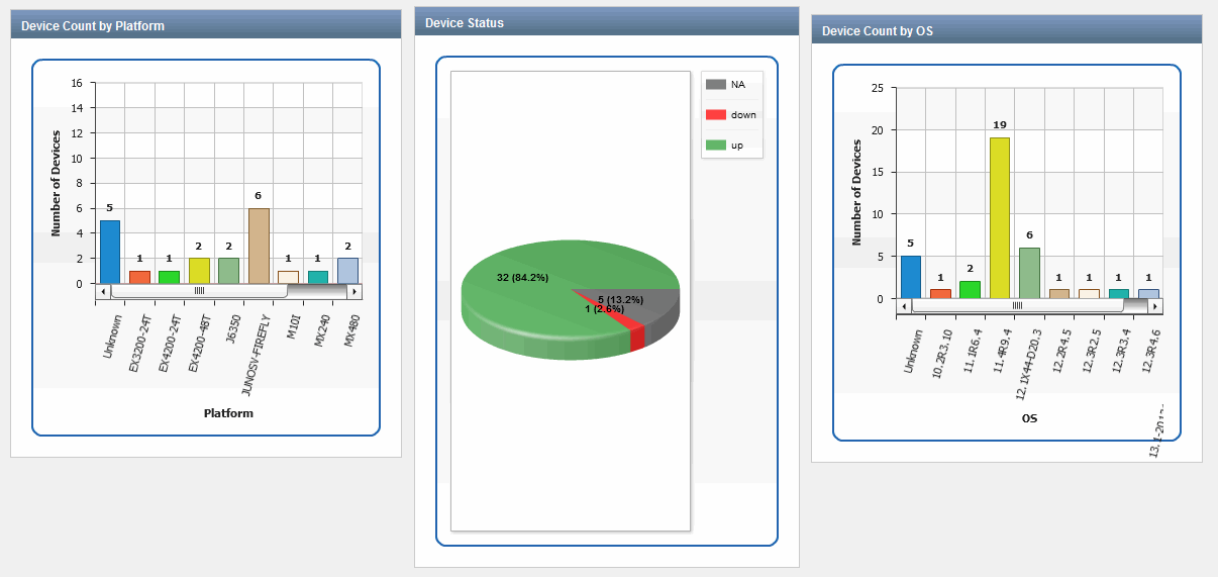
Use the task tree on the left side of the page to navigate application workspaces and perform tasks within a workspace. When you select an application from the **Applications** list (at the top left of the Junos Space UI), all the workspaces for the selected application are displayed in the task tree.

If you know the workspace in which you want to perform an action (task), select the workspace from the task tree on the left side of the page. The right side of the page displays information about the selected workspace and its objects.

Workspace Statistics

When you select the name of a workspace from the task tree, Junos Space Network Management Platform displays high-level statistics representing the status of managed objects in that workspace. The statistics and charts displayed for different workspaces are different. Figure 38 shows the charts displayed on the Devices workspace statistics page.

Figure 38: Workspace Statistics Pages



If a chart has more data points than can be viewed clearly simultaneously, a scroll bar appears at the bottom or side of the chart.

If you click a bar or pie-chart segment, you navigate to the corresponding inventory page, filtered according to the bar or segment you selected. For example, if you click the MX240 devices bar on the Device Count by Platform bar chart, you navigate to the Devices > Device Management inventory page, which in this

case displays all the MX240 devices on the network that are discovered and managed by Junos Space Network Management Platform.

You can move the charts and graphs on the page or resize them.

You can also print or save the statistics by right-clicking the graphic (bar chart or pie chart) and selecting the appropriate option.

RELATED DOCUMENTATION

Junos Space User Interface Overview | 89

Inventory Landing Page Overview

IN THIS SECTION

- Organizing Your View | 130
- Working with Objects on an Inventory Page | 134
- Exporting Data | 135

In the Junos Space Network Management Platform UI, you navigate to an inventory page by selecting an application, expanding an application workspace, then selecting a management task. For example, to view the Device Management inventory page, select **Devices** > **Device Management**.

The inventory pages display information related to managed objects for a particular task group or task in tabular format. The fields that are displayed are different for different inventory pages, depending on the task group that you selected.

For each managed object, specific data associated with it is stored in the Junos Space Platform database. For example, in the case of devices, device name, interfaces, OS version, platform, IP address, connection, managed status, and so on are stored.

Inventory pages enable you to view and manipulate managed objects individually or collectively. Managed objects include devices, logs, users, jobs, clients, software, licenses, and so on. You can organize your view to display only those objects that you want to see, in the way that you want to see them.

You can select an object or objects by selecting the check box to the left of each object on the inventory page. You can select one, several, or all objects and perform actions on them using the shortcut menu or the Actions menu. Selecting the check box to the left in the first column of the column header row selects or deselects all items. The objects that you select and on which you perform an action remain selected.

> **NOTE:** The function and implementation of individual inventory pages depends on the Junos Space Platform application design.

Organizing Your View

IN THIS SECTION

- Paging Controls | **131**
- Sorted-by Indicator | **131**
- Show or Hide Columns | **132**
- Filter Submenus | **133**

Before you start working on data that is displayed on various inventory landing pages (ILPs), it would be best to organize your view on the ILP so that Junos Space presents you with only the information that you need. The following sections provide information about how you can organize your view.

Paging Controls

Figure 39 shows the paging controls that appear at the bottom of the inventory page. You can use these controls to browse the inventory when the inventory is too large to fit on one page.

Figure 39: Page Information Bar

The **Page** box lets you jump to a specific page of the inventory. Type the page number in the **Page** box and press **Enter** to jump to that page. The **Show** box enables you to customize the number of objects displayed per page. Table 11 describes other table controls.

Table 11: Table Paging and Refreshing Controls

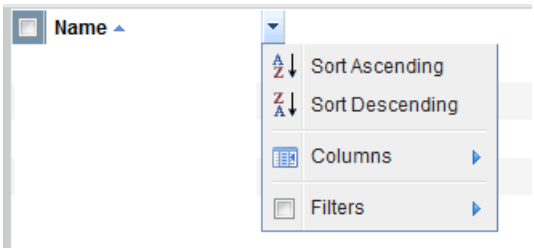
Page Control	Operation
	Advances to the next page of the table
	Returns to the previous page of the table
	Displays the last page of the table
	Displays the first page of the table
	Refreshes the table content

Sorted-by Indicator

The sorted-by indicator is a small arrowhead next to a column name. It displays how the objects are sorted in a column. When you sort a column, the column name is highlighted and the indicator appears.

You can sort inventory data using the **Sort Ascending** and **Sort Descending** commands on the column header drop-down menu. Click the down arrow on a table header to view the menu. In Figure 40, the device inventory is sorted by the Name column.

Figure 40: Sorting Tables

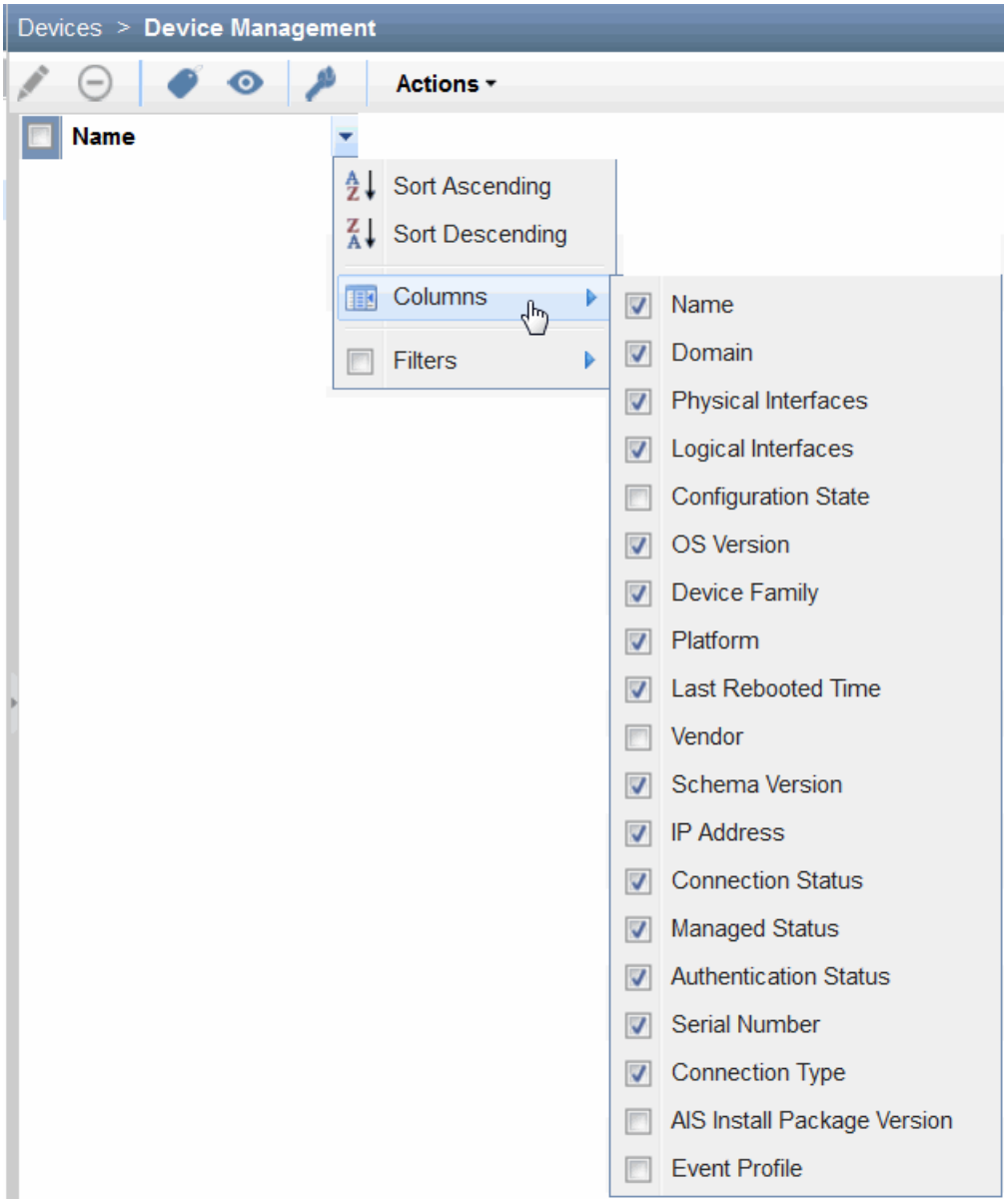


Some columns do not support sorting.

Show or Hide Columns

You can show or hide columns on the inventory page by selecting or not selecting the column name on the Columns cascading menu, as shown in Figure 41. All column header drop-down menus have this option. Only the columns that are selected appear in the inventory table.

Figure 41: Showing or Hiding Columns in Tables



Filter Submenus

For information about filtering options in Junos Space Platform Release 17.2R1 and later, see "Filter Management in Junos Space Platform User Interface" on page 137.

Working with Objects on an Inventory Page

IN THIS SECTION

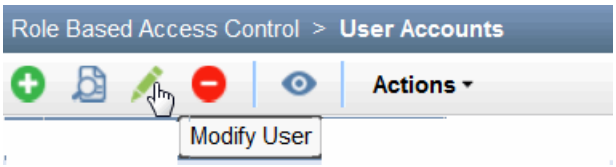
- Toolbar Icons | 134
- Actions Menu and Shortcut Menu | 134

To initiate an action on the objects that are available on an inventory page, you can use:

Toolbar Icons

Almost all inventory landing pages provide a toolbar containing icons that provide easy access to frequently used tasks. While some icons are common across inventory landing pages such as the **Display Quick View** icon (which displays a small window summarizing data about the selected object), most icons are specific to an inventory landing page. For example, in Figure 42, the Modify User icon is specific to the User Accounts inventory landing page.

Figure 42: Toolbar Icons



Actions Menu and Shortcut Menu

You can perform actions on one or more selected items on an inventory page by using the Actions menu, or by right-clicking the items to invoke the shortcut menu. To use the Actions menu, select one or more objects, select an action or subgroup of actions from the Actions menu. (Note that the subgroup has an arrowhead next to its name.) For example, to view the physical interfaces of a device, select that device on the **Device Management** inventory page, open the Actions menu, expand the **Device Inventory** subgroup, and select **View Physical Inventory**.

You can also select one or more items on the inventory page, then right-click. The shortcut menu appears and you can select an action or subgroup of actions.

NOTE: If you are using Mozilla Firefox earlier versions, the Advanced JavaScript Settings might disable the shortcut menu.

To ensure that you can use the shortcut menu:

1. In Mozilla Firefox, select **Tools** > **Options** to display the Options dialog box.
2. In the Options dialog box, click the **Content** tab.
3. Click **Advanced** to display the Advanced JavaScript Settings dialog box.
4. Select the **Disable or replace context menus** option.
5. Click **OK** in the Advanced JavaScript Settings dialog box.
6. Click **OK** in the Options dialog box.

If you are using newer versions of Mozilla Firefox, it may not be necessary to perform the preceding steps. By default, you need not change any of the Firefox settings. But, if you have changed the settings or for some reason the shortcut menus do not appear properly, then you need to perform the following steps in the recent versions:

1. **Disable or replace context menus**—Deselect this option to prevent webpages from disabling or changing the Firefox shortcut menu.
2. In **about:config(URL): dom.event.contextmenu.enabled**, set it to false to block sites. The default value is true.

Exporting Data

You can export data that is displayed on certain inventory landing pages such as the MD5 Validation Result inventory page (in the Images workspace) as well as export job details pertaining to certain tasks initiated from Junos Space Platform. For example, you can export job details related to device discovery, staging and deployment of device images, and so on.

NOTE: Not all jobs in Junos Space support the export of job details.

The data is exported as a comma-separated file (CSV) to your computer, allowing you to process the data offline. For example, you can use this data to identify devices on which staging or deployment of an image failed.

To export the data that is displayed on the MD5 Validation Result page as a CSV file:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Images**.

   The Images page displays the list of device images.

2. Select a device image.

3. Select **MD5 Validation Result** from the Actions menu.

   The MD5 Validation Result page displays the results of verification tasks.

4. Click **Export to CSV** from the Actions menu.

   You are prompted to save the file.

5. Click **OK** on the File Save dialog box to save the file to your local file system.

6. After you save the file, to return to the MD5 Validation Result page, click the [X] icon on the **Exporting Validation Results** dialog box to close it.

Navigate to the location where you saved the file and open the file by using an application such as Microsoft Excel. If you are opening this file as an Excel workbook, then filter the data for the **Failed** status in the **Checksum Result** column to identify devices in which the images are not staged completely. From the filtered data, see the **Device Image Name** column to obtain information about the images that are not staged completely.

To export the image deployment job details as a CSV file:

1. On the Junos Space Platform UI, select **Jobs** > **Job Management**.

2. Double-click the image deployment job whose details you want to export as a CSV file.

3. Click **Export as CSV**.

   You are prompted to save the file.

4. Click **OK** on the File Save dialog box to save the file to your local file system.

5. To return to the Job Management page, click **OK** on the **Exporting Device Image Job** dialog box.

Use an application such as Microsoft Excel to open the downloaded file from your computer. If you are using Microsoft Excel, you can filter data in the **Status** column to identify the devices on which the deployment of images failed.

RELATED DOCUMENTATION

Junos Space User Interface Overview | 89

Filter Management in Junos Space Platform User Interface

IN THIS SECTION

- Understanding Filtering Options in Junos Space Platform User Interface | 137
- Managing Filtering Options | 150
- Error Conditions and Error Messages for Filters | 158

This section contains the following topics:

Understanding Filtering Options in Junos Space Platform User Interface

IN THIS SECTION

- Overview | 138
- Benefits | 139
- Pages and Columns that Support Filtering | 139

This topic contains the following sections:

Overview

On various Junos Space Platform pages, you can use the **Filter** menu to show or hide table entries based on the filtering criteria that you specify. Filters enable you to quickly find and evaluate the entries that are relevant to your specific needs.

Many of the columns in Junos Space page tables support filtering. To know whether or not a column supports filtering of data, click the down arrow next to the column name. If the **Filter** submenu appears, then that column supports filtering of data. The filtering criteria that are available for you depend on the selected column. You can create filters that combine criteria from more than one column.

From Release 17.2R1 onward, Junos Space Platform introduces the following enhancements to filtering options:

- Ability to save, modify, and delete filters
- Ability to share saved filters with other users
- Ability to mark filters as favorites
- Ability to manually enter filter conditions with autocomplete and suggestion support.

For a list of pages and columns that support filtering, see "Pages and Columns that Support Filtering" on page 139.

In releases earlier than 17.2R1, Junos Space Platform supports only basic filtering. In those releases, you can specify only one set of filter criteria at a time, and the filter setting is lost when you modify the criteria. From Junos Space Platform Release 17.2R1 onward, you can save multiple filters. You can also mark up to 10 filters as favorites in each of the pages that support enhanced filtering.

The Filter menu that appears when you click the filter icon lists up to 10 filters. The 10 filters that are listed in the Filter menu are arranged in the following order of filter categories: favorite filters, public filters, and private filters. If there are more than 10 filters, those filters are listed under the More Filters submenu.

> **NOTE:** The **More Filters** submenu is not displayed if you have not saved any filter. However, the **More Filters** submenu appears even if you have saved only one filter.

If you have Filter Management permissions to create or modify filters, you can also choose to share the saved filters with other users by marking the filters as public.

For more information about creating, saving, modifying, and deleting filters, see "Managing Filtering Options" on page 150.

From Junos Space Platform Release 17.2R1, you can also manually enter filter criteria in the filter text box that appears when you click the **Show/ Clear and Hide Filters** option from the Filter menu. For more

information about manually specifying filter criteria, see “Creating Filters by Manually Entering the Filter Criteria” on page 150.

Benefits

Filters enable you to quickly find and evaluate the entries that are relevant to your specific needs. Ability to save and share filters enables you to configure multiple filters for a page that can be preserved across sessions and shared with multiple users.

Pages and Columns that Support Filtering

IN THIS SECTION

- Pages and Columns that Support Enhanced Filtering | **140**
- Pages That Support Basic Filtering | **149**

This section contains the following topics:

Pages and Columns that Support Enhanced Filtering

The following table lists the pages and columns that support enhanced filtering and also the data types for each of the columns:

Page	Column	Data Type
Device Management	Name	String
	Device Alias	String
	IP Address	Number
	Serial Number	String
	Connection Status	List
	Managed Status	List
	Platform	String
	OS Version	String
	Domain	String
	Device Family	String
	Configuration State	List
	Last Rebooted Time	Date
	Vendor	String
	Authentication Status	String
	Aggregation Device	String
	Satellite Devices	String
	Device Network	List

Page	Column	Data Type
View Physical Interfaces	Physical Interface Name	String
	IP Address	String
	IPv6 Address	String
	MAC Address	String
	Operational Status	List
	Admin Status	List
	Link Level Type	String
	Link Type	String
	Speed	String
	MTU	String
	Description	String
	Domain	String
View Logical Interfaces	Interface Name	String
	IP Address	String
	IPv6 Address	String
	Description	String
	Domain	String
Device Discovery Profiles	Profile Name	String
	Target Type	List
	Target Details	String
	Profile Visibility	List
	Job ID	Number

Page	Column	Data Type
Model Devices	Name	String
	Description	String
	Devices Count	Number
Device Adapter	Name	String
	Device Family	String
	Version	String
	Adapter State	List
Template Definitions	Name	String
	Domain	String
	Description	String
	Last Modified By	String
Templates	Name	String
	Domain	String
	Template Type	List
	Latest Version	String
	Description	String
	Last Modified By	String
	Deployment Status	List

Page	Column	Data Type
Configlets	Name	String
	Domain	String
	Category	String
	Device Family Series	List
	Latest Version	String
	Git Version	String
	Git Branch	String
	Execution Type	List
	Creation Time	Date
	Last Updated Time	Date
	Last Modified By	String
	Reference Number	Number
Configuration View	Name	String
	Domain	String
	Title	String
	Device Family Series	List
	View Type	List
	Creation Time	Date
	Last Updated Time	Date
	Last Modified By	String

Page	Column	Data Type
Configuration Filter	Name	String
	Domain	String
	Device Family Series	List
Xpath and Regex	Name	String
	Domain	String
	Value	String
	Property Type	List
	Creation Time	Date
	Last Updated Time	Date
	Last Modified By	String
Images	File Name	String
	Domain	String
	Version	String
	Type	List

Page	Column	Data Type
Scripts	Script Name	String
	Domain	String
	Descriptive Name	String
	Type	List
	Category	String
	Execution Type	String
	Format	List
	Latest Revision	String
	Git Version	String
	Git Branch	String
Operations	Operation Name	String
	Domain	String
	Description	String
	Creation Time	Date
	Last Updated Time	Date
Script Bundles	Script Bundle Name	String
	Domain	String

Page	Column	Data Type
Config Files Management	Config File Name	String
	Device Name	String
	Device Alias	String
	Latest ConfigFile Version	String
	Creation Date	Date
	Last Updated Date	Date
Job Management	ID	Number
	Domain	String
	Name	String
	Percent	Number
	State	List
	Job Type	String
	Parameters	String
	Summary	String
	Scheduled Start Time	Date
	Actual Start Time	Date
	End Time	Date
	Owner	String
	Retry Group Id	Number
	Previous Retry	Number

Page	Column	Data Type
User Accounts	User Name	String
	First Name	String
	Last Name	String
	Email	String
	User Type	List
	Status	List
	GUI/API Access	List
	Locked Out	List
Roles	Role Title	String
	Type	List
	Description	String
User Sessions	User Name	String
	IP Address	String
	Fabric Node Name	String
	Session Start Time	Date

Page	Column	Data Type
Audit Log	ID	Number
	User Name	String
	User IP	String
	Domain	String
	Application	String
	Task	String
	Timestamp	Date
	Result	String
	Description	String
	Job ID	Number
Fabric	Last Monitored Time	Date
	Last Boot Time	Date
Audit Log Forwarding	Name	String
	Description	String
	Server Address	String
	Port	Number
	Protocol	List
	Last Updated User	String
	Last Updated Time	Date
	Enabled	List

Page	Column	Data Type
Tags	Name	String
	Owner	String
	Description	String
	Access Type	List
Report Definitions	Name	String
	Domain	String
	Created By	String
	Created Time	Date
	Description	String
Generated Reports	Name	String
	Generated Time	Date
	Domain	String
	Description	String
	Definition Name	String
	Generated By	String
	Format	String
	Job ID	Number

Pages That Support Basic Filtering

Junos Space Platform supports basic filtering options on the following pages:

- Role Based Access Control > Domains
- Administration > CA/CRL Certificates
- Administration > SMTP Servers
- Administration > DMI Schemas

NOTE: Filtering is supported only for the State and Schema Installed columns.

SEE ALSO

Managing Filtering Options | 150

Error Conditions and Error Messages for Filters | 158

Managing Filtering Options

IN THIS SECTION

- Creating Filters by Manually Entering the Filter Criteria | 150
- Creating Filters by Using the Filter Submenu Options | 153
- Saving a Filter | 155
- Modifying a Filter | 155
- Creating a Public Filter | 156
- Applying a Filter | 157
- Clearing a Filter | 157
- Deleting a Filter | 157

From Junos Space Platform 17.2R1 onward, you can save filters, modify the saved filters, and delete the filters. You can also mark the filters as public or favorites or both. The following sections explain the various filter management tasks that you can perform from the Junos Space Platform user interface (UI):

Creating Filters by Manually Entering the Filter Criteria

From Junos Space Platform Release 17.2R1 onward, you can manually enter the filtering criteria to create the filters that meet your specific requirements.

To manually enter filtering criteria:

1. From any of the pages that support Filter Management options, click the **Filter** icon.

   The Filter menu appears.

2. Click **Show/ Clear and Hide Filters** on the Filter menu.

   The Filter field appears.

3. Click inside the **Filter** field.

   A list showing the names of columns that support filtering and the following two options appears:

   - An opening parenthesis [**(**] symbol. The bracket enables you to group conditions. A closing parenthesis [**)**] symbol appears in the list after you specify a condition if you used an opening parenthesis before specifying the condition.
   - **Not**. The Not option enables you to specify conditions based on which you want to filter out entries.

4. From the list, select the columns for which you want to specify the filter conditions and specify the conditions by using any of the operators supported for the specified column. Table 12 lists various operators that you can use for each of the data types supported for filtering.

   You can specify multiple conditions by using an AND or an OR operator. The Filter field supports autocomplete and provides suggestions for column names, attributes, and operators even as you type inside the field.

   NOTE: If the values you enter for any of the parameters contain spaces, enclose such values in single quotation marks. For example, **Domain Contains 'test domain'**. However, if the single quotation mark is part of the search string, use the backslash escape character (\) before the quotation mark. For example: **Domain Contains '\'test domain\''**.

Table 12: Data Types and Supported Operators

Data Type	Supported Operators
String (Other than Domain Column)	Starts-with
	Ends- with
	Contains
	=
	!=

Table 12: Data Types and Supported Operators *(continued)*

Data Type	Supported Operators
String (Domain Column only)	Contains
	Not-contains
Numbers or Date	=
	!=
	>
	<
	<=
	>=
List	=
	!=

The following examples show samples of manually entered filter criteria:

- **ID > 2000000 AND 'Job Type' ends-with 'elements' AND Parameters contains '1.1.1.1' OR Parameters = 192.168.27.72 AND Owner = SUPER**

  This filter on the Job page displays jobs that meet the following criteria: The job ID is a number greater than 2000000, the job type ends with the text elements, the Parameter field contains 1.1.1.1 or 192.168.27.72, and the owner is the superuser.

- **('Connection Status' = 'down') AND ('Managed Status' = 'In Sync' OR 'Managed Status' = Synchronizing) AND 'Device Family' starts-with 'junos'**

  This filter on the Device page displays devices that have the connection status set to down, the managed status set to in sync or synchronizing, and device family name starts with Junos.,

5. After you enter the conditions, you can save or apply the filter. To save the filter, click the **Save Filter** icon and complete the steps as explained in "Saving a Filter" on page 155. To apply the filter without saving, click the **Apply Filter** icon. For more information about applying filters, see "Applying a Filter" on page 157.

   To clear the filter conditions you entered or the filter that you applied, click the **Clear Filter** icon. Alternatively, you can click the **Clear and and Hide** icon to clear the filters and hide the filter bar.

For a list of error messages, see “Error Conditions and Error Messages for Filters” on page 158.

Creating Filters by Using the Filter Submenu Options

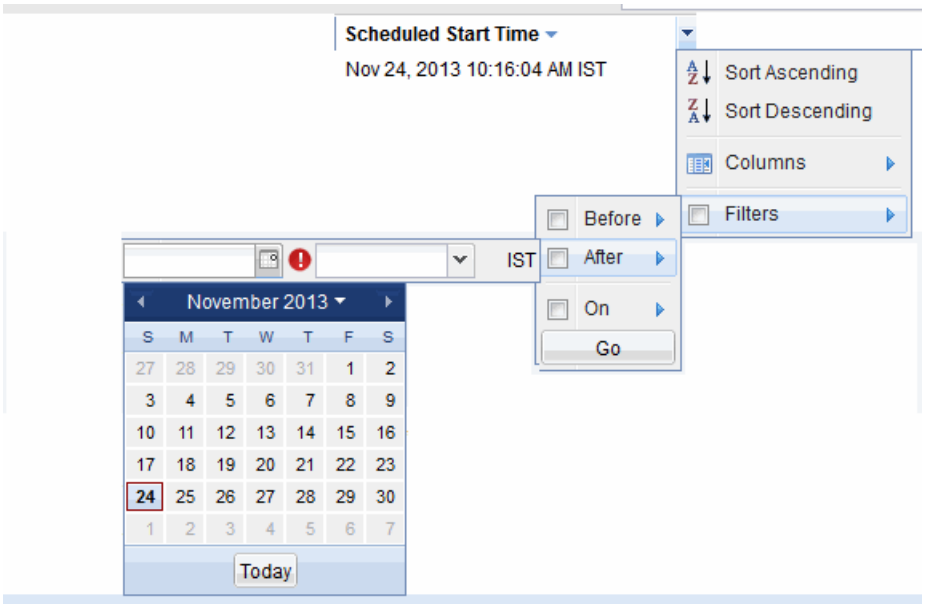
Many of the columns in Junos Space user interface tables support filtering. To know whether or not a column supports filtering of data, click the down arrow next to the column name. If the **Filter** submenu appears, then that column supports filtering of data. The criteria that are available for you to filter on depend on the selected column. You can create filters that combine criteria from more than one column.

On Junos Space pages that support enhanced filtering options, the Filter field and the **Save Filter**, **Apply Filter**, and **Clear Filter** icons appear when you select any of the items from the Filter submenu. The selected criteria are displayed in the Filter field. You can choose to apply, save, or clear the filtering criteria by clicking the appropriate icon.

On Junos Space pages that do not support enhanced filtering options, when you select any of the items from the Filter submenu, Junos Space Platform displays the filter criteria, including the columns being filtered, above the table. Junos Space Platform displays a red **X** to the left of the filter criteria above the table. You can clear the filter and restore the table to its original view by clicking the **X**.

Figure 43 shows a typical Filter submenu for a date column.

Figure 43: Typical Submenu for a Date Column



The following procedures describe how to use the different types of available filters.

To filter entries on the Junos Space pages:

1. On the Junos Space Platform UI, click the down arrow on the column header and select **Filters**.

   The Filters submenu appears, displaying the list of operators or values that you can select, based on the type of values in the column.

2. Based on the submenu that appears, perform one of the following procedures.

   To specify filters for a date field:

   a. From the Filter submenu, select **Before**, **After**, or **On**.

      You can select both **Before** and **After** dates and times to filter the entries by a specific time period. You can also select **On** to view events recorded on a specific date.

   b. Click the calendar icon and select the date from the calendar.

      You can click **Today** to view the events that occurred today at the specified time.

   c. Click the arrow beside the time list and select the time.

   To specify filters for a text field:

   a. In the text box that appears, type the alphanumeric string based on which you want to filter entries.

   To specify filters for a field with discrete values such as **Success** or **Failure**, or **True** or **False**:

   a. From the list of values that appears, select the check boxes for one or more values based on which you want to filter entries.

   To specify filters for a numeric field:

   a. Enter values for each operator that you want to specify.

3. Click **Go** to view the entries filtered based on the criteria that you specified.

4. On pages that support enhanced filtering options, you can choose to save the filter after you specify the required criteria. To save the filter, click the **Save Filter** icon and complete the steps as explained in "Saving a Filter" on page 155. To apply the filter without saving, click the **Apply Filter** icon. For more information about applying filters, see "Applying a Filter" on page 157.

   To clear the filter conditions you entered or the filter that you applied, click the **Clear Filter** icon.

You can also filter entries based on combined filters with different criteria specified for different columns. For example, you can filter for all events on a certain date whose status was *success*. When you use multiple filters, the filters are joined using the logical AND operator.

To clear only the part of a filter that applies to a any of the columns, click the down arrow on the column header and clear the check box next to **Filter**.

Saving a Filter

You can create a filter either by using the filtering options that are available in the Junos Space Platform UI or by manually entering the filter criteria in the Filter field that appears when you click the **Filter** icon. After you specify the filtering criteria, you can save the filter.

To save a filter:

1. Create a filter as explained in either of the following topics:
   - Creating Filters by Manually Entering the Filter Criteria on page 150
   - Creating Filters by Using the Filter Submenu Options on page 153

   The criteria you specified, either by typing in the Filter field or by using the Filter submenu options in the Junos Space Platform UI, appear in the Filter field.

2. Click the **Save Filter** icon next to the **Filter** field.

   The Save Filter page appears.

3. In the Name field, enter a name for the filter.

4. (Optional) In the Description field, enter a description for the filter.

5. (Optional)To share the filter with other users, select the **Make Public** check box.

   NOTE: You cannot change a public filter to a private filter after you save the changes. However, you can change a private filter to a public filter from the Modify Filters page.

6. (Optional) If you want to mark the filter as a favorite, select the **Mark as Favorite** check box.

   Alternatively, you can add a filter to the list of favorites or remove a filter from the list of favorites from the Manage Filters page.

7. Click Save to save the filter. To close the page without saving the filter, click Cancel.

Modifying a Filter

From the Manage Filters page. you can modify saved filters.

1. From the Junos Space Platform UI, go to the page that contains the filter that you want to modify. For example, the Device Management or View Physical Devices page.

2. Click the **Filter** icon to view the Filter menu.

3. From the Filter menu, click **Manage Filters**.

   The Manage Filters page appears.

4. From the list of filters, click the filter entry that you want to modify.

   The selected filter entry appears highlighted.

5. Modify the following parameters as required:

   - Name–The name of the filter.
   - Description–Description for the filter.
   - Filter Criteria–Filter criteria to apply for the filter. For information about manually entering the filter criteria, see "Creating Filters by Manually Entering the Filter Criteria" on page 150.
   - Make Public–Specify whether the filter is a public filter. Public filters are available for all users. However, note that only users with Filter Management permissions to create or modify filters can create public filters. This check box is disabled if the selected filter is a Public filter. That is, you cannot clear this check box after you select this check box and save the filter.

     NOTE: To create a public filter, you must have both Create Filter and Modify Filter roles assigned to your account.

   - Mark as Favorite–Specify whether the filter is a favorite or not. You can select this check box to mark the selected filter as favorite. To remove a filter from the list of favorites, clear this check box. Favorite filters are listed on top of the Filter menu options. If there are favorite filters and filters that are not marked as favorites, the filters that are not marked as favorites appear in the **More Filters** submenu.

6. Click **Modify** to save the changes. Click **Reset** if you want to discard the changes.

For a list of error messages, see "Error Conditions and Error Messages for Filters" on page 158.

Creating a Public Filter

Public filters are filters that are available to all users. To create a public filter, you must have both Create Filter and Modify Filter roles assigned to your account. Junos Space Platform adds the suffix *(Public)* to the names of filters that are made public.

To make a filter public:

1. When you save a filter, select the **Make Public** check box. For more information about saving filters, see "Saving a Filter" on page 155.

2. When you modify a filter, select the **Make Public** check box. For more information about modifying filters, see "Modifying a Filter" on page 155

> **NOTE:** After you make a filter public, you cannot change that to a private filter.

Applying a Filter

Junos Space Platform provides you multiple options to apply a filter.

- From pages that support enhanced filtering, you can apply a filter by clicking the name of the filter from the **Filter** menu. Alternatively, while creating a filter, you can click the **Apply Filter** icon (the green tick mark) next to the Filter field.
- From pages that do not support enhanced filtering, you can apply a filter by selecting and specifying filter options from the **Filter** submenu available for columns that support filtering and then clicking **Go**.

Clearing a Filter

Junos Space Platform provides you the following options to clear a filter that is applied to a page.

- On Junos Space pages that support enhanced filtering options, if a filter is applied to the page, the filter criteria is displayed in the Filter field. You can click the **Clear Filter** icon to clear the applied filter. Alternatively, you can click the **Clear and Hide Filters** icon from the Filter bar or the **Show/Clear and Hide** item in the Filter menu.
- On Junos Space pages that do not support enhanced filtering options, when you select any of the items from the Filter submenu, Junos Space Platform displays the filter criteria, including the columns being filtered, above the table. Junos Space Platform displays a red **X** icon to the left of the filter criteria above the table. You can clear the filter and restore the table to its original view by clicking the **X** icon.

Deleting a Filter

From the Manage Filters page. you can delete saved filters.

To delete a saved filter:

1. From the Junos Space Platform UI, go to the page that contains the filter that you want to delete. For example, the Device Management or View Physical Devices page.

2. Click the **Filter** icon to view the Filter menu.

3. From the **Filter** menu, click **Manage Filters**.

   The Manage Filters page appears.

4. From the list of filters, click the filter entry that you want to delete.

   The selected filter entry appears highlighted.

5. Click the **Delete** icon above the top-left corner of the list of filters.

   The Delete Filter page appears.

6. On the Delete Filter page, click **OK**. Click **Cancel** if you do not want to delete the selected filter.

SEE ALSO

Understanding Filtering Options in Junos Space Platform User Interface | 137

Error Conditions and Error Messages for Filters | 158

Error Conditions and Error Messages for Filters

The following table lists common error conditions you might encounter while saving or applying filters and the error messages for those conditions:

Table 13: Error Conditions and Error Messages for Filters

Error Condition	Sample Filter Data	Validation Error Message at Apply Filter	Validation Error Message on the Save Filter and Manage Filter Page
Invalid column name.	'namm'	Invalid column name: namm	Invalid filter query

Table 13: Error Conditions and Error Messages for Filters *(continued)*

Error Condition	Sample Filter Data	Validation Error Message at Apply Filter	Validation Error Message on the Save Filter and Manage Filter Page
Incorrect filter query. Comparison missing after column name.	'Name' juniper 'Name' has test OR 'Device Alias' contains test	Incorrect filter query, please provide a comparison after column name (Name)	Invalid filter query
Incorrect filter query. Value after comparison missing.	Name = Name = juniper OR Name =	Incorrect filter query, please provide a value after comparison (=)	Invalid filter query
Incorrect filter query; “)” missing.	(Name = test	Incorrect filter query, please insert ")" to complete the query (test)	Invalid filter query
Incomplete filter query. Column name or "(" missing.	(Name = juniper) OR	Incomplete filter query. Please provide a column name or "(" to complete the query after (OR)	Invalid filter query
Incomplete filter query. Column name or "(" missing after (NOT)	(Name = juniper) OR NOT	Incomplete filter query. Please provide a column name or "(" to complete the query after(NOT)	Invalid filter query
Incorrect filter query; Unexpected token ")"	Name = test)	Incorrect filter query, Unexpected token ")"	Invalid filter query

Table 13: Error Conditions and Error Messages for Filters *(continued)*

Error Condition	Sample Filter Data	Validation Error Message at Apply Filter	Validation Error Message on the Save Filter and Manage Filter Page
Incorrect filter query; Unexpected token ")"	Name = test AND (Name = test1))	Incorrect filter query, Unexpected token ")"	Invalid filter query
Incorrect filter query; Unexpected token "("	Name = test AND (Name = test1)(	Incorrect filter query, Unexpected token "("	Invalid filter query
Incorrect filter query; ")" missing.	(Name = test AND (Name = test1)	Incorrect filter query, please insert ")" to complete the query (test)	Invalid filter query
Invalid filter query. Query must start with "(" or NOT or column name.	)	Invalid filter query. Query should start with "(" or NOT or column name.	Invalid filter query
Invalid filter query	(Name starts-with ")	Invalid filter query. Query should start with "(" or NOT or column name.	Invalid filter query
The equal condition is not supported for the specified column.	Domain = SUCCESS		Filtering of “Domain” column is not possible with “Equal” condition
The not equal condition is not supported for the specified column.	Domain != SUCCESS		Filtering of “Domain” column is not possible with “Not Equal” condition

Table 13: Error Conditions and Error Messages for Filters *(continued)*

Error Condition	Sample Filter Data	Validation Error Message at Apply Filter	Validation Error Message on the Save Filter and Manage Filter Page
The greater than condition is not supported for the specified column.	Name > Test	Filtering of “Name” column is not possible with “Greater than” condition	Filtering of “Name” column is not possible with “Greater than” condition
The less than condition is not supported for the specified column.	Name < Test	Filtering of “Name” column is not possible with “Less than” condition	Filtering of “Name” column is not possible with “Less than” condition
The “greater than or equal to” condition is not supported for the specified column.	Name >= Test	Filtering of “Name” column is not possible with “Greater than or equal to” condition	Filtering of “Name” column is not possible with “Greater than or equal to” condition
The “Less than or equal to” condition is not supported for the specified column.	Name <= Test	Filtering of “Name” column is not possible with “Less than or equal to” condition	Filtering of “Name” column is not possible with “Less than or equal to” condition
The “contains” condition is not supported for the specified column.	ID contains 123	Filtering of “ID” column is not possible with “contains” condition	Filtering of “ID” column is not possible with “contains” condition

Table 13: Error Conditions and Error Messages for Filters *(continued)*

Error Condition	Sample Filter Data	Validation Error Message at Apply Filter	Validation Error Message on the Save Filter and Manage Filter Page
The “not-contains” condition is not supported for the specified column.	ID not-contains 123	Filtering of “ID” column is not possible with “not-contains” condition	Filtering of “ID” column is not possible with “not-contains” condition
The “starts-with” condition is not supported for the specified column.	ID starts-with 123	Filtering of “ID” column is not possible with “starts-with” condition	Filtering of “ID” column is not possible with “starts-with” condition
The “ends-with” condition is not supported for the specified column.	ID ends-with 123	Filtering of “ID” column is not possible with “ends-with” condition	Filtering of “ID” column is not possible with “ends-with' condition
The specified column supports only numbers for values.	ID = test	“ID” column accepts only Numbers	“ID” column accepts only Numbers
The input value is not supported for the specified column.	'Device Network' = 123	“Device Network” column can not be filtered with the provided filter value “123”	“Device Network” column can not be filtered with the provided filter value “123”
The input date and time value does not match the supported format.	'End Time' = 10pm	“End Time” column accepts only valid date, Example: 11/03/2017 01:14AM	“End Time” column accepts only valid date, Example: 11/03/2017 01:14AM

Table 13: Error Conditions and Error Messages for Filters *(continued)*

Error Condition	Sample Filter Data	Validation Error Message at Apply Filter	Validation Error Message on the Save Filter and Manage Filter Page
The input value is not supported for the specified column.	State = SUCCES	“State” column can not be filtered with the provided filter value “SUCCES”	“State” column can not be filtered with the provided filter value “SUCCES”
The input column name is invalid or is of a column for which filtering is not supported.	State = SUCCESS		Column name “State is invalid or Filtering of that column is not supported.

SEE ALSO

Understanding Filtering Options in Junos Space Platform User Interface | 137

Managing Filtering Options | 150

Global Search Overview

The global search field on the Junos Space Network Management Platform UI helps you to quickly locate objects within Junos Space Platform. When you search for an object by using global search, Junos Space Platform performs a full-text search operation for objects within Junos Space Platform, and displays the matches found.

The search results are filtered on the basis of your Role-Based Access Control (RBAC) permissions, such as the tasks that a user is allowed to perform and the domains to which a user is assigned. For example, users are shown results only for tasks for which they have the appropriate permissions or results related to domains to which the users are assigned. For more information about RBAC permissions, see the "Role-Based Access Control Overview" on page 995 topic (in the *Junos Space Network Management Platform Workspaces User Guide*).

The search is performed and the results are displayed based on how the Junos Space Platform objects are indexed. Table 14 lists the indexed objects on which you can perform a search operation by using the global search feature.

Junos Space Platform monitors its database at regular intervals to identify new objects that need to be indexed. The default interval is set to five seconds.

NOTE:

- An administrator can configure the refresh interval from the Administration workspace. For more information about configuring the refresh interval, see the **Index auto update interval in seconds** parameter in "Modifying Junos Space Network Management Platform Settings" on page 1346 (in the *Junos Space Network Management Platform Workspaces User Guide*).
- An administrator can also refresh the search index manually from the Administration workspace by navigating to **Administration** > **Applications** > **Network Management Platform** and selecting **Refresh Search Index** from the Actions menu.

Table 14: Searchable Objects

Object Category	Indexed Fields (Category) and Description
Device	• name—Name of the device. • deviceFamily—Device family of the device. • platform—Hardware platform. • os—Junos OS version of the device. • ip—Device management IP address. • connectionStatus—Device connection state, which indicates whether the device is up or down. • managedStatus—Device management status, such as “In Sync,” “Connecting,” “Sync Failed,” and so on. • serialNumber—Serial number of the device. • ccState—Candidate configuration state of the device, such as “Created,” “Accepted,” or “Rejected”. • vendor—Name of the device vendor. • authenticationStatus—Indicateshow the device is connected to Junos Space, such as “Credential Based,” “Key based,” or “Key Conflict.” Credential-based uses username and password for connection; whereas, key-based needs an RSA key for establishing a connection. The UI displays key conflict when the keys on Junos Space and device are not the same. • connectionType—Connection type of the device.
Physical interface	• name—Name of the physical interface. • ip—Assigned IP address of the physical interface. • mac—MAC address of the physical interface. • operationStatus—Operational status of the physical interface (up or down). • adminStatus—Administrative status of the physical interface (up or down). • linkLevelType—Link level type of the physical interface. • linkType—Link type of the physical interface, such as full-duplex or half-duplex. • speed—Link speed on the physical interface. • mtu—MTU of the physical interface. • description—Description of the physical interface.
Logical interface	• name—Name of the logical interface. • ip—IP address of the logical interface. • encapsulation—Encapsulation on the logical interface, such as VLAN-VPLS. • vlanId—Assigned VLAN number of the logical interface. • description—Description of the logical interface.

Table 14: Searchable Objects *(continued)*

Object Category	Indexed Fields (Category) and Description
Device physical inventory	• name—Name of the module. • version—Software release version of the module. • modelNumber—Model number of the module. • model—Device family of the module. • partNumber—Part number of the module. • serialNumber—Serial number of the module. • status—Status of the module. • description—Description of the module
Software inventory	• model—Model of this device. • routingEngine—Routing engine of the device. • name—Name of the installed software package. • version—Version number of the installed software package. • type—Type of the installed software package. Permitted values are operating-system, internal-package, and extension. • major—Major portion of the version number. For example, in version 13.1R1.14, the major portion is 13. • minor—Minor portion of the version number. For example, in version 13.1R1.14, the minor portion is 1. • revisionNumber—Revision number of the package. For example, in version 13.1R1.14, the revision number is 1.14. • description—Description of the installed software package
Tags	name—List of tags assigned to an object

Table 14: Searchable Objects *(continued)*

Object Category	Indexed Fields (Category) and Description
Audit log	• userName—Name of the user who performed an action that generated this audit log entry. For example, when userA logs in to Junos Space Network Management Platform, an audit log entry is generated to record the login activity. When you search for userA, this audit log entry is displayed as part of the search results. • userIpAddr—IP address from which the action was performed. • taskName—Action that was performed by the user, such as Login, Logout, and so on. • timeStamp—Date and time of action. • executionResult—Result of the action, such as Success, Job Scheduled, and so on. • description—Description of the action, such as Login Succeeded, Logout Succeeded, and so on. • jobId—Job ID of the action that was performed. **NOTE:** Not all actions trigger a job. • recId—Audit log ID.
Job	• jobId—Job ID. • name—Name of the job. • percent—Percentage of job completed at a given instant,such as 30, 100, and so on. • state—Indicates whether the job is a success, failure, or in progress. • jobType—Type of job. • scheduledStartTime—Date and time at which the job is scheduled to start. • actualStartTime—Date and time at which the job actually started. • endTime—Date and time at which the job was completed. • owner—Name of the user who triggered the job. • retryGroupId—Job ID of the original job. • previousRetry—Job ID of the previous job. • parameter—Objects on which a job is performed or is scheduled to be performed. • summary—Operations executed for the job.

Table 14: Searchable Objects *(continued)*

Object Category	Indexed Fields (Category) and Description
Configlets	• configletsName—Name of the configlet. • configletsCategory—Category specified by a user at the time of creation or modification of a configlet. • configletsDeviceFamilySeries—Family of the device. • configletsLastestVersion—Latest version of the configlet. • configletsDescription—Description of the configlet specified by a user at the time of creation or modification of a configlet. • configletsExecutionType—Type of execution of the configlet—single or grouped. • configletsCreationTime—Time at which the configlet was created. • configletsLastUpdatedTime—Time at which the configlet was last updated. • configletsLastModifiedBy—Name (login ID) of the user who last modified the configlet. • referenceNumber—Reference number of the configlet, which a user has provided during creation or modification of the configlet.
Configuration View	• configurationViewName—Name of the configuration view • configurationViewTitle—Title of the configuration view • configurationViewDeviceFamilySeries—Family of the device. • configurationViewDescription—Description of the configuration view specified by a user at the time of creation or modification of a configuration view • configurationViewOrder—Order in which the configuration view must be applied • configurationViewType—Type of configuration view—Form view, Grid view, XML view, and CLI view • configurationViewCreationTime—Time at which the configuration view was created • configurationViewLastUpdatedTime—Time at which the configuration view was last updated • configurationViewLastModifiedBy—Name (login ID) of the user who last modified the configuration view

Table 14: Searchable Objects *(continued)*

Object Category	Indexed Fields (Category) and Description
Scripts	• scriptName—Name of the script file • scriptDescriptiveName—Descriptive name of the script that is mentioned within the script • scriptType—Type of script—Commit Script, Op Script, and Event Script • scriptExecutionType—Type of execution—Device (script with this execution type should be staged on to a device before it can be executed) and Local (script with this execution type can be executed without having to stage it on a device) • scriptFormat—Format of the script file (XSL and SLAX) • scriptLatestRevision—Latest version number of the script • scriptCreationDate—Time at which the script was imported to the Junos Space server • scriptDescription—Description of the script • scriptLastUpdatedTime—Time at which the script was last updated • deviceNameList—Devices with which a script is associated
Templates	• name—Name of the device template • currentVersion—Current version of the device template • description—Description of the device template • modifiedBy—Name (login ID) of the user who last modified the device template • modifiedTime—Time at which the template was last updated • state—Device template deployment readiness (Needs Review, Disabled, or Enabled) • deployStat—Deployment status of the template (assigned, created, or deployed) • type—Type of device template (configuration template or quick template) • deviceFamily—Supported device family of this device template"
Template Definition	• name—Name of the template definition. • description—Description of the template definition. • deviceFamily—Supported device family of the template definition. • state—State of the template definition. • schemaVersion—Schema version of the template definition. • modifiedBy—User who last modified user the template definition. • modifiedTime—Time that the template definition was last modified.

Table 14: Searchable Objects *(continued)*

Object Category	Indexed Fields (Category) and Description
Xpath and Regex	• xpathRegexName—Name of the regular expression or XPath • xpathRegexValue—XPath or regex value. For example: [a-zA-Z0-9], /device/configuration/interfaces/interface/unit, or /device/configuration/interfaces/interface[name="$INTERFACE.get(0)"]/unit/name/text() • xpathRegexPropertyType—Property type—Regular Expression, XPath Context, or XPath Search • xpathRegexCreationTime—Time at which the XPath or regular expression was created • xpathRegexLastUpdatedTime—Time at which the XPath or regular expression was last updated • xpathRegexLastModifiedBy—Name (login ID) of the user who last modified the XPath or regular expression
Images	• imagesFileName—Filename of the device image. For example, **jinstall-ex-4200-12.3R4.6-domestic-signed.tgz** • imagesVersion—Version of the device image • imagesSeries—Series supported by the device image • deviceNameList—Devices on which the device image is deployed
Report Definitions	• name—Name of the report definition • reportDefintionsCreatedBy—Name (login ID) of the user who created the report definition • reportDefinitionsCreatedTime—Time at which the report definition was created • reportDefinitionsDecription—Description of the report definition
Generated Reports	• name—Name of the generated report • generatedReportsGeneratedTime—Time at which the report was generated • generatedReportsDescription—Description of the generated report • generatedReportsDefinitionName—Name of the report definition using which the report was generated • generatedReportsGeneratedBy—Name (login ID) of the user who generated the report • generatedReportsFormat—Format of the generated report • generatedReportsJobId—ID of the job associated with report generation

Table 14: Searchable Objects *(continued)*

Object Category	Indexed Fields (Category) and Description
Configuration Files	• name—Name of the configuration file, which is the device serial name with the **.conf** file extension • configFileDeviceName—Name of the device whose configuration file is backed up • lastestConfigFileVersion—Latest version number of the backup configuration file • configFileCreationDate—Time when the configuration file was created on the Junos Space server. It corresponds to the time at which you back up a device configuration for the first time from the Junos Space server. • configFileLastUpdatedDate—Time at which the device configuration was last modified
User Accounts	• userName—Login ID of the Junos Space user • userFirstName—First name of the Junos Space user • userLastName—Last name of the Junos Space user • userEmail—E-mail ID of the Junos Space user • userType—Type of the user—local, remote, or read only • userStatus—Status of the user—enabled or disabled • passwordStatus—Status of the password—active or expired • lockedOut—Whether the user is locked out or not • roleType—Whether the user has access to the UI, API, or both

NOTE:

- If you are searching for entries in Junos Space Platform on the basis of the date or time field, the correct search results are not returned if the comma (,) or the colon (:) characters are part of the search string.

  For example, to search for Nov 10, 2016 6:21:33 AM, enter the following search string: **Nov 10 2016 6 21 33 AM**. An exact match is returned if found; otherwise, merged results that match any of the parts of the search string are returned. In this example, if an exact match, Nov 10, 2016 6:21:33 AM, is not found, the search results will return all entries that match any of the space-separated parts of the search string, for example, Nov 9, 2016 7:37:21 AM, Jun 10, 2016 6:21:14 PM, and Nov 4, 2015, 2:12:45 PM.

- Date and time search works only if both the Junos Space server and the user executing the search are in the same time zone.

The global search operation also supports query expressions. You can search for phrases and multiple terms. The default operator for multiple terms is the OR operator.

NOTE:

When you enter a query expression, be aware of the following:

- You must add a back slash "\" if you want to use the following special characters in the search text:

  + && || ! ( ) { } [ ] ^ " ~ * ? : \

- Field names are case-sensitive. To search within a specific field, the search syntax is: "*<Indexed field or column name>:<search text>*"

  For example, if you have a few systems running on Junos OS 12.3 Release 4.5, then "os: 12.3R4.5" returns search results, whereas "OS: 12.3R4.5" does not return search results. This is because the field name that is indexed is "os" and not "OS." Another example to search for information pertaining to the Junos EX Series devices is to enter "deviceFamily:junos-ex" in the Search field.

- If you want to search for a term that includes a space, enclose the term within double quotation marks.

  For example, to search for all devices that are synchronized (that is, In Sync), enter "In Sync" in the Search field.

- You must append "*" if you want to search using partial keywords. Otherwise, the search returns 0 (zero) matches or hits.

Table 15 provides examples of query expressions that you can enter in the **Search** field.

Table 15: Query Expressions in the Search Field

Query Expression	Matches Objects That Contain
snmp	snmp
snmp ntp	snmp or ntp
snmp OR ntp	snmp or ntp
snmp AND ntp	snmp and ntp
protocol:snmp	snmp in the protocol field
protocol:snmp AND NOT subject:snmp	snmp in the protocol field but not in the subject field
(snmp OR ntp) AND http	http and the terms—snmp or ntp

Table 15: Query Expressions in the Search Field *(continued)*

Query Expression	Matches Objects That Contain
description:“http server”	Exact phrase “http server” in the description field
description: “http server”~5	http and server within five positions of one another in the description field (that is, http and server need to have no more than 5 words in-between them)
ge-*	Terms that begin with “ge-,” such as ge-0/0/1 or ge-0/0/1.4
s??p	Terms such as smtp or snmp
lastmodified:[1/1/2012 TO 12/31/2012]	Last modified field values between the dates January 1, 2012 and December 31, 2012
port:(80 8080 8888)	80, 8080, or 8888 in the port field
IPAddress:10.1.1.1	10.1.1.1 or 10.1.1.0/24 in the IPAddress field

RELATED DOCUMENTATION

Junos Space User Interface Overview | 89

Using Global Search | 173

Using Global Search

You can use the global search feature of Junos Space Network Management Platform to find objects within Junos Space Platform.

To search for objects using the global search feature:

1. In the **Search** field, located at the top of the Junos Space Platform UI, type the search criteria and press **Enter**. (Alternatively, you can click the magnifying glass icon adjacent to the Search field.)

   If none of the objects in Junos Space Platform match your search criteria, the following error message is displayed:
   No matching results were found. Please enter different search criteria.

   If any of the objects match the search criteria, the results appear on the search results page, which is divided into two areas. The area on the left displays the filters that you can use to refine your search results, and the area on the right displays the search results with a short description about each result.

   The search criteria that you typed are highlighted in the search results. Each search result may also provide a URL to help you navigate to the corresponding object on the inventory landing page.

   > **NOTE:** When the search results are displayed, an informational message about how to hide the search results is displayed in a dialog box.
   >
   > Perform one of the following actions:
   >
   > - To prevent the informational message from appearing again, ensure that the **Don't show again** check box is selected and click **OK**. The **Don't show again** check box is selected by default.
   > - To allow the informational message to continue appearing, clear the **Don't show again** check box and click **OK**.

2. (Optional) Click the URL provided with the search result to navigate to the inventory landing page of the desired object.

3. (Optional) To filter the search results, select the relevant category or subcategories displayed on the left of the search results page.

4. (Optional) To view the previous search results, click **View Last Search Results**. However, if this is your first search after logging in to Junos Space, then this link is not displayed.

5. To dismiss the search results page or to navigate to the inventory landing page from which you performed the search, click one of the following:

   - The **Hide Search Results** button
   - The left navigation tree or any of the global action icons
   - The close [X] button on the top-right of the search results panel

RELATED DOCUMENTATION

Junos Space User Interface Overview | 89

Global Search Overview | 164

Viewing Your Jobs

You can view all your completed, in-progress, canceled, failed, and scheduled jobs in Junos Space Network Management Platform. Your jobs include jobs that were triggered by you as well as jobs that were reassigned to you. The My Jobs icon on the banner of the Junos Space Platform UI, allows you to quickly access summary and detailed information about all your jobs, from any workspace and from any task that you are currently performing.

To view your jobs:

1. In the banner of the Junos Space Platform UI, click the **My Jobs** icon located at the top right.

   The My Jobs dialog box appears, displaying your 25 most recent jobs.

   For each job, the following information is displayed:

   - Job ID
   - Job name
   - Job status
   - Date and time—The date and time displayed depends on the status of the job:
     - For jobs that are in progress, the date and time at which the job started are displayed.
     - For failed jobs, the date and time when the job failed are displayed.
     - For successful jobs, the date and time when the job succeeded are displayed.
     - For jobs that are scheduled for later, the date and time at which the job is scheduled to run are displayed.
   - Percentage of the job completed

2. (Optional) To view all your jobs, click **Manage My Jobs**.

   The Job Management page appears and displays a list of all your jobs.

3. (Optional) To view the details of a specific job, click the *job ID*.

   The Job Management page appears and displays the details of the selected job in a dialog box.

4. Click **Close** to exit the My Jobs page.

For troubleshooting, see the **/var/log/jboss/servers/server1/server.log** file.

RELATED DOCUMENTATION

- Viewing Statistics for Jobs | **968**
- Canceling Jobs | **985**
- Jobs Overview | **965**
- Clearing Your Jobs | **986**

Changing Your Password on Junos Space

After you log in to Junos Space Network Management Platform, you can change your password using the User Settings icon on the Junos Space banner. You do not require any particular Junos Space role to change your password. After a password change, you are logged out of the application. You must login again with the new password. If you use REST API to change the password, you must use Basic Auth to change the password, instead of using session ID or cookies.

Starting with Junos Space Platform Release 12.1, Junos Space has implemented a default standard for passwords that is compliant with the industry standard for security.

NOTE:

- When you upgrade to Junos Space Platform Release 12.1 or later, the default standard takes effect immediately. All local users receive password expiration messages the first time they log in to Junos Space after the update.
- You need to have set your local password to be able to change it. If you do not have a local password set, you will not be able to set or change it.
- You can use the **User Settings** icon to change only your local password. The change does not affect any passwords that an administrator might have configured for you on a remote authentication server.

To change your local password:

1. On the Junos Space Platform UI, click the **User Settings** icon on the right side of the Junos Space banner.

   The **Change User Settings** dialog box appears.

2. In the **Old Password** text box, enter your old password.

   NOTE: Mouse over the information icon (small blue *i*) next to the **New Password** text box to view the rules for password creation. For more information about the password rules, see "Modifying Junos Space Network Management Platform Settings" on page 1346.

3. In the **New Password** text box, enter your new password.

4. In the **Confirm Password** text box, enter your new password again to confirm it.

> **NOTE:** The fields on the **X.509 Certificate** tab are applicable when you want to use certificate-based authentication. If you are using password-based authentication, you can ignore these fields. For more information about certificate-based authentication, see the "Certificate Management Overview" on page 1426 topic in the *Junos Space Network Management Platform Workspaces Feature Guide*.

5. (Optional) Select the **Manage objects from all assigned domains** check box on the **Object Visibility** tab to view and manage objects from all the domains that you are assigned to.

6. Click **OK**.

   You are logged out of the system. To log in to Junos Space again, you must use your new password. Other sessions logged in with the same username are unaffected until the next login.

RELATED DOCUMENTATION

Logging In to Junos Space | 100

Junos Space User Interface Overview | 89

Logging Out of Junos Space

After you complete your administrative tasks in the Junos Space UI, log out to prevent unauthorized users from accessing Junos Space.

- To log out of Junos Space, click the **Log Out** icon on the Junos Space application banner.

The logout page appears. A user who is idle and has not performed any action, such as keystrokes or mouse-clicks, is automatically logged out of Junos Space after a specified amount of time. This setting conserves server resources and protects the system from unauthorized access. The default setting is 5 minutes of inactivity. You can change the setting on the Applications inventory page. Select **Administration** > **Applications** > **Network Management Platform** > **Modify Application Settings** (from the Actions menu) > **User** > **Automatic logout after inactivity (minutes)** to modify the automatic logout setting.

To log in to the system again, click the **Click here to log in again** link on the logout page.

RELATED DOCUMENTATION

Logging In to Junos Space | 100

Junos Space User Interface Overview | 89

Workspaces User Guide

1

PART

Overview

Introduction | **182**

CHAPTER 6

Introduction

IN THIS CHAPTER

- Junos Space Platform Workspaces Overview | 182
- Viewing the Junos Space Platform Dashboard | 184

Junos Space Platform Workspaces Overview

In Junos Space Network Management Platform, the different tasks that you can perform are categorized into *workspaces*. The task tree on the left side of a Junos Space Platform page is expanded by default and displays the different Junos Space Platform workspaces and the tasks that you can perform in each workspace.

> **NOTE:** When you log in to Junos Space, the **Applications** list displays **Network Management Platform** by default. You can expand this list to see the installed Junos Space applications.

You can collapse the task tree to the left by clicking the double left arrow (**<<**) button and expand the task tree by clicking the double right arrow (**>>**) button.

The first item in the task tree is **Dashboard**, which provides you access to the Junos Space Platform Dashboard page. After this, the list of the workspaces available in Junos Space Platform are displayed; these workspaces are described at a high level in Table 5.

> **NOTE:** If you select a Junos Space application from the **Applications** list, the task tree for that application is displayed. This topic describes the workspaces for Junos Space Platform; for the tasks in Junos Space applications, refer to the documentation for Junos Space applications.

You can expand any workspace by clicking the expansion symbol (**+**) to the left of its name. When you do so, the next level of the tasks for that workspace is displayed; some items at the second level might contain further sub-tasks.

You can expand as many workspaces or tasks as you like; previously-expanded ones remain open until you collapse them. The design of the task tree enables you to easily navigate across the different Junos Space Platform workspaces and tasks.

Table 16: Junos Space Platform Workspaces

Workspace Name	Description
Devices	Manage devices, including adding, discovering, importing, and updating them. For more information, see "Device Management Overview" on page 189.
Device Templates	Create configuration definitions and templates used to deploy configuration changes on multiple Juniper Networks devices. For more information, see "Device Templates Overview" on page 462.
CLI Configlets	CLI Configlets are configuration tools provided by Junos OS that allow you to apply a configuration to a device easily. For more information, see "CLI Configlets Overview" on page 534.
Images and Scripts	Deploy, verify, enable, disable, remove, and execute scripts deployed to devices. For more information, see "Scripts Overview" on page 673. Download a device image from the Juniper Networks Software download site to your local file system, upload it into Junos Space, and deploy it on one or more devices simultaneously. For more information, see "Device Images Overview" on page 613.
Reports	Generate customized reports for managing network resources. For more information, see "Reports Overview" on page 768.
Network Monitoring	Perform fault monitoring and performance monitoring of managed devices and fabric nodes. For more information, see "Network Monitoring Workspace Overview" on page 799.
Configuration Files	Maintain backups of device configuration in the Junos Space Platform database. For more information, see "Managing Configuration Files Overview" on page 938.

Table 16: Junos Space Platform Workspaces *(continued)*

Workspace Name	Description
Jobs	Monitor the progress of ongoing jobs. For more information, see "Jobs Overview" on page 965.
Role Based Access Control	Add, manage, and delete users, custom roles, domains, and remote profiles, and manage user sessions. For more information, see "Configuring Users to Manage Objects in Junos Space Overview" on page 1033.
Audit Logs	View and filter system audit logs, including those for user login and logout, tracking device-management tasks, and displaying services that were provisioned on devices. For more information, see "Junos Space Audit Logs Overview" on page 1115.
Administration	Add network nodes, back up your database, manage licenses and applications, or troubleshoot. For more information, see "Junos Space Administrators Overview" on page 1136, "Maintenance Mode Overview" on page 1153, and other topics related to the Administration workspace.

RELATED DOCUMENTATION

Viewing the Junos Space Platform Dashboard | 126

Viewing the Junos Space Platform Dashboard

When you log in to Junos Space Network Management Platform, the home page is displayed. By default, the home page for Junos Space Platform is the Dashboard page. However, if you previously configured a different page as the home page, then the configured home page is displayed when you log in.

The Junos Space Platform dashboard, as shown in Figure 37, displays graphs that provide information about the overall system condition, the fabric load history, the active users history, and the percentage of jobs in different states. The charts are visible to all users and are updated in real time.

NOTE: If you do not have user privileges to view detailed data, you might not be able to view detailed information if you select a gadget.

Figure 44: Junos Space Platform Dashboard Page

To access the Junos Space Dashboard page:

1. On the Junos Space Platform UI, select **Dashboard**.

   The Dashboard page is displayed.

2. (Optional) To view more information related to the overall system condition, click **Overall System Condition** or the indicator needle.

   You are taken to the Fabric page, where you can view detailed information about the nodes in the fabric. For more information, see "Viewing Nodes in the Fabric" on page 1186.

3. (Optional) To view information related to the fabric load, on the **Fabric Load History** graph:

   - Mouse over a graph data point to view the average CPU usage percentage.
   - Click the blue line depicting the CPU usage to view detailed information.

     You are taken to the Fabric page, where you can view detailed information about the CPU, memory, and disk usage for the nodes in the fabric.

4. (Optional) To view information related to the active users, on the **Active Users History** graph:

   - Mouse over a graph data point to view the total number of active users at that point.
   - Click a data point on the graph to view more information about the active users at that point.

     You are taken to the User Accounts page, where the active users are displayed. For more information, see "Viewing User Statistics" on page 1068.

5. (Optional) To view information related to the jobs, on the **Job Information** graph:

   - Mouse over a segment in the pie chart to view the percentage of jobs with a particular status; for example, cancelled jobs, successful jobs, or failed jobs.
   - Click a segment of the pie chart to view details of jobs with status corresponding to the segment.

     You are taken to the Job Management page, where the jobs filtered by the status are displayed. For more information, see "Viewing Jobs" on page 972.

6. (Optional) You can view records about the health and performance of the Junos Space nodes in your Junos Space setup and the processes on these nodes in a system health report. The health and performance data collected from the nodes is displayed in the System Health Report table. For more information, see "Viewing the Administration Statistics" on page 1138.

7. (Optional) You can move any chart displayed on the Dashboard page by clicking inside the title bar and dragging the chart.

8. (Optional) You can resize any chart displayed on the Dashboard page by hovering over an edge and clicking and dragging the edge.

RELATED DOCUMENTATION

Junos Space Platform Workspaces Overview | **182**

Overall System Condition and Fabric Load History Overview | **1159**

2

PART

Devices

Device Management | **189**

Systems of Record | **214**

Device Discovery Profiles | **220**

Modeling Devices | **246**

Device Authentication in Junos Space | **281**

Viewing Device Inventory | **299**

Exporting Device Inventory | **312**

Configuring Juniper Networks Devices | **321**

Device Adapter | **371**

Device Configuration Management | **376**

Adding and Managing Non Juniper Networks Devices | **386**

Accessing Devices | **391**

Logical Systems (LSYS) | **417**

Device Partitions | **422**

Custom Labels | **426**

Verifying Template, Image Deployment, Script Execution, and Staged Images on Devices | **434**

Device Monitoring | **441**

Device Maintenance | **446**

CHAPTER 7

Device Management

IN THIS CHAPTER

- Device Management Overview | 189
- Confirmed-commit from Junos Space Network Management Platform | 191
- Viewing Managed Devices | 194
- Juniper Networks Devices Supported by Junos Space Network Management Platform | 199
- Uploading Device Tags by Using a CSV File | 211
- Filtering Devices by CSV | 212

Device Management Overview

IN THIS SECTION

- Managed and Unmanaged Devices | 190
- IPv4 and IPv6 Address Support | 191

The Devices workspace in Junos Space Network Management Platform simplifies the management of devices in your network. You use the device discovery profile or model device workflows to add multiple devices to the Junos Space Platform database. Then you can perform the following tasks to manage, configure, and monitor the devices from the Devices workspace:

- View the connection status and managed status of the managed devices.
- View the operational and administrative status of the physical interfaces of the devices.
- View the hardware inventory of a selected device, such as information about power supplies, chassis cards, fans, Flexible PIC Concentrators (FPCs), and available PIC slots.
- Change the mode to authenticate the devices.

- View, modify, and deploy the configuration to the devices. For example, deploy a service order to activate a service on your managed devices.
- Execute scripts on and apply CLI Configlets to the devices.
- View information about the scripts associated with or executed on the devices and the device images staged on the devices.
- Access the devices from the Junos Space user interface and execute commands on the devices.
- If the network is the system of record, resynchronize a managed device with the Junos Space Network Management Platform database so that both the device and the database contain the same device configuration. (If Junos Space Network Management Platform is the system of record, this capability is not available.)
- View statistics about the managed devices in your network, including the number of devices by platform and the number of devices by Junos OS release.
- Clone the devices.
- Reboot the devices.
- Monitor and troubleshoot problems on the devices.

This topic describes the following:

Managed and Unmanaged Devices

With Junos Space Platform, you can add the following types of devices to the Junos Space Platform database:

- Managed devices–Managed devices are Juniper Networks devices running Junos OS. For more information about Juniper Networks devices supported on Junos Space Platform, refer to "Juniper Networks Devices Supported by Junos Space Network Management Platform" on page 199.

  Juniper Networks devices, such as MX480 and MX960 routers running as aggregation devices, display the number of satellite devices to which the aggregation device is connected and the mode of the aggregation device (that is, single-home or multihome). For more information about inventory and interfaces, see "Device Inventory Overview" on page 299. For more information about aggregation devices, satellite devices, and Junos Fusion technology, refer to the *Junos Fusion* documentation.
- Unmanaged devices–Unmanaged devices are non-Juniper Networks devices. Junos Space Platform displays the IP addresses and hostnames of unmanaged devices. The managed status of unmanaged devices is Unmanaged. The device status in several columns is displayed as NA. For more information, refer to "Viewing Managed Devices" on page 194. For information about adding unmanaged devices to Junos Space Network Management Platform, see "Adding Unmanaged Devices" on page 386.

IPv4 and IPv6 Address Support

Junos Space Platform supports both IPv4 and IPv6 addresses for the following device management tasks:

- Discovering devices
- Adding unmanaged devices
- Creating connection profiles and modeling devices
- Connecting to devices through Secure Console
- Uploading RSA keys to devices

> **NOTE:** The IP addresses that you input for these tasks either manually or by using a CSV file are validated on the basis of the format of the IP address.

RELATED DOCUMENTATION

- Device Discovery Profiles Overview | 220
- Device Inventory Overview | 299
- Systems of Record in Junos Space Overview | 214
- DMI Schema Management Overview | 1534
- Understanding How Junos Space Automatically Resynchronizes Managed Devices | 216
- Junos Space IPv6 Support Overview | 1152

Confirmed-commit from Junos Space Network Management Platform

Junos Space Network Management Platform supports the Junos OS confirmed-commit functionality. By default, Junos Space Platform uses confirmed-commit for all commit operations on all devices that are discovered on Junos Space Platform and that support the confirmed-commit NETCONF capability. The default timeout value for the confirmed-commit operations issued by Junos Space Platform is 10 minutes. Junos Space Platform sends a remote procedure call (RPC) for confirmed-commit immediately after sending the RPC for a commit. The devices stay connected even if the commit operation contains an incorrect configuration edit that may disconnect the device from Junos Space Platform. An EJB callback method is used to verify the change in configuration on the device.

A candidate configuration created using the Schema-based Configuration Editor and Configuration Guides support the confirmed-commit functionality. If you are deploying the configuration by using a template,

you need to publish these templates to the candidate configuration of the device. When you push the configuration to the devices by using the Schema-based Configuration Editor, templates, or the Configuration Guide, the job triggered for these tasks display the timeout value of confirmed-commit. Job details include the time taken for the EJB callback method to return a value and the time taken to confirm the commit operation or perform a rollback operation.

Table 17 lists the managed status of the device in NSOR and SSOR modes when a candidate configuration is deployed to a device that supports the confirmed-commit NETCONF capability. It also lists the status of the job details when the confirmed-commit operation is a success or failure in these modes.

Table 17: Managed Status in NSOR and SSOR Modes for confirmed-commit

Confirmed-commit and EJB Callback Method Success and Failure Conditions	NSOR Mode	SSOR Mode	Job Result and Details
Junos Space Platform issues a confirmed-commit operation with a timeout value.	In Sync	Space Changed	NA
An EJB callback is sent to the device to verify the change in configuration on the device.	NA	NA	NA
The EJB callback method does not return any value within the confirmed-commit timeout interval.	In Sync	Space Changed	Failed
The EJB callback method returns True and the commit is confirmed.	Out Of Sync followed by resynchronization by Junos Space Platform	In Sync or Space Changed (if new changes are added to the candidate configuration)	Success
The EJB callback method returns False and the configuration is rolled back.	Out Of Sync followed by resynchronization by Junos Space Platform	Space Changed	Failure with the **failed callback** error
The EJB callback method returns False and the device is automatically rolled back to the currently active configuration.	Out Of Sync followed by resynchronization by Junos Space Platform	Space Changed, Device Changed (after Junos Space Platform receives the system log about the auto-rollback operation on the device)	Failure with auto-rollback details

NOTE: In SSOR mode, if a confirmed-commit is not successful and if the device is automatically rolled back, you need to manually accept the change by using the Resolve Out-of-band Changes workflow to change the managed status of the device to In Sync.

NOTE: If a device is disconnected from Junos Space Platform (that is, Connection Status is down) after Junos Space Platform issues a confirmed-commit and is automatically rolled back before connecting back to Junos Space Platform, you need to manually check the device configuration from the CLI to confirm that the commit operation was successful.

RELATED DOCUMENTATION

- Viewing the Configuration Change Log | **381**
- Viewing Managed Devices | **194**
- Reviewing and Deploying the Device Configuration | **327**

Viewing Managed Devices

You can view details of all managed devices in your network, such as the operating system, platform, IP address, license, and connection status. Device information is displayed in a table. Unmanaged devices are also shown, but without status and some other information.

You can also view devices that are in the managed status from the Network Monitoring workspace, through the Node List (see "Viewing the Node List" on page 809). If the network is the system of record, you can resynchronize your managed devices with the Junos Space Platform database (see "Resynchronizing Managed Devices with the Network" on page 448).

Neither manual nor automatic resynchronization occurs when Junos Space Network Management Platform is the system of record. See "Systems of Record in Junos Space Overview" on page 214.

To view configuration and runtime information of managed devices:

1. On the Network Management Platform UI, select **Devices > Device Management**.

   The Device Management page is displayed.

   Figure 45 shows the Device Management page.

Figure 45: Device Management Page

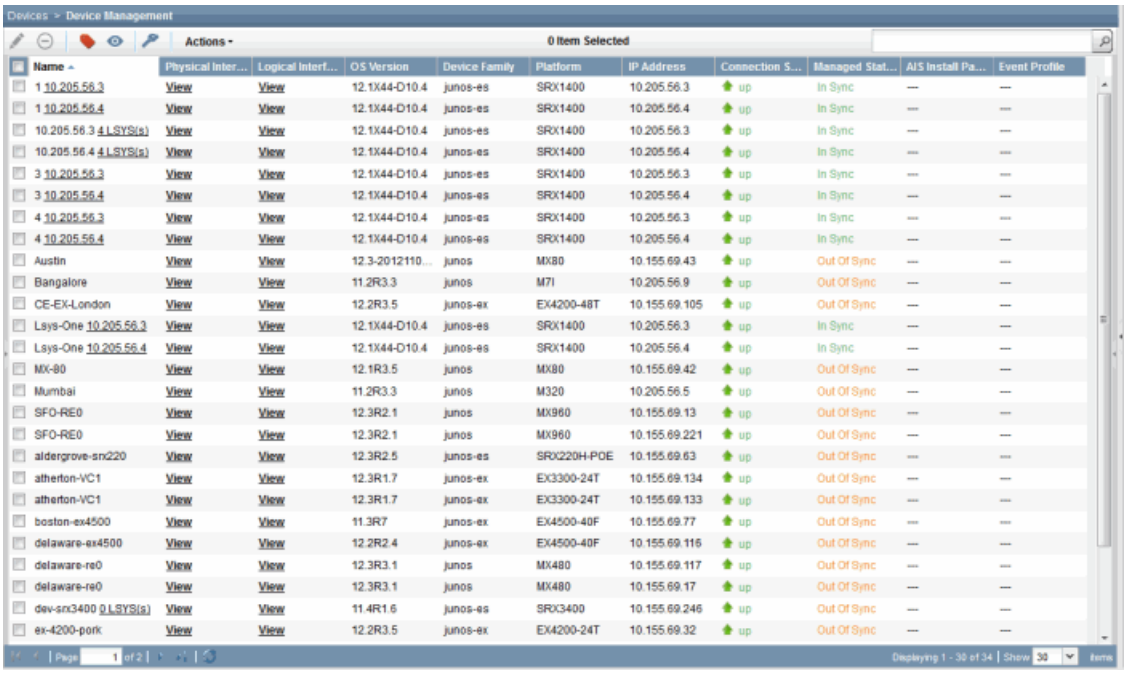


Table 18 describes the fields displayed on the inventory page. In the table, an asterisk against a field name indicates that the field is not shown by default.

Table 18: Fields in the Device Management Table

Field	Description
Name	Name of the device as stored in the Junos Space Platform database
Device Alias	Value of the Device Alias custom label for the device. By default, this field is not displayed on the page. (This field is empty if the Device Alias custom label is not added or no value is assigned to the Device Alias custom label for the device.)
IP Address	IPv4 or IPv6 address of the device
Serial Number	Serial number of the device chassis (This field displays Unknown for an unmanaged device.)
Connection Status	Connection status of the device in Junos Space Platform. Different values are displayed in network as system of record (NSOR) and Junos Space as system of record (SSOR) modes. • up—The device is connected to Junos Space Platform. When the connection status is up, in NSOR mode, the managed status is Out Of Sync, Synchronizing, In Sync, or Sync Failed. In SSOR mode, the status is In Sync, Device Changed, Space Changed, Both Changed, or Unknown (which usually means connecting). • down—The device is not connected to Junos Space Platform. When the Connection status is down, the managed status is None or Connecting. • NA—The device is unmanaged.

Table 18: Fields in the Device Management Table *(continued)*

Field	Description
Managed Status	Current status of the managed device in Junos Space Platform: • Connecting—Junos Space Platform has sent a connection remote procedure call (RPC) and is waiting for the first connection from the device. • In Sync—The synchronization operation has completed successfully; Junos Space Platform and the device are synchronized with each other. • None—The device is discovered, but Junos Space Platform has not yet sent a connection RPC. • Out Of Sync—In NSOR mode, the device has connected to Junos Space Platform, but the synchronization operation has not been initiated, or an out-of-band configuration change on the device was detected and auto-resynchronization is disabled or has not yet started. • Device Changed—In SSOR mode, there are changes made to the device configuration from the device CLI. • Space Changed—In SSOR mode, there are changes made to the device configuration from Junos Space Platform. • Space & Device Changed—In SSOR mode, there are changes made to the device configuration from the device CLI and Junos Space Platform. Neither automatic nor manual resynchronization is available. • Synchronizing—The synchronization operation has started as a result of device discovery, a manual resynchronization operation, or an automatic resynchronization operation. • Sync Failed—The synchronization operation failed. • Unmanaged—The device is unmanaged. • Modeled—The device is modeled. • Waiting for deployment—The modeled device is unreachable and needs to be activated.
Platform	Model number of the device (For an unmanaged device, the platform details are discovered through SNMP. If the platform details cannot be discovered, the field displays Unknown.)
OS Version	Operating system firmware version running on the device (This field displays Unknown for an unmanaged device.)
Schema Version	DMI schema version that Junos Space Platform uses for this device (This field displays Unknown for an unmanaged device.) See “DMI Schema Management Overview” on page 1534.
Physical Interfaces	Link to the view of physical interfaces for the device (The field displays NA for an unmanaged device.)

Table 18: Fields in the Device Management Table *(continued)*

Field	Description
Logical Interfaces	Link to the view of logical interfaces for the device (The field displays NA for an unmanaged device.)
Device Family	Device family of the selected device (For an unmanaged device, this is the same as the vendor name you provided. The field displays Unknown if no vendor name was provided and if SNMP is not used or has failed.)
Configuration State	Current state of the device configuration: • NA – No change is made to the configuration. This is the default state. • Created – A change is made to the device configuration from Junos Space Platform. • Approved – The device configuration is approved. • Rejected – The device configuration is rejected.
Last Rebooted Time	Date and time when the device was last rebooted manually (that is, the device status changes from Down to Up) or from Junos Space Platform
Vendor	Name of the device vendor (For an unmanaged device, the field displays Unknown if the vendor name was not provided and cannot be discovered through SNMP.)
Authentication Status	• Key Based—The authentication key was successfully uploaded. • Credential Based—A key upload was not attempted; log in to this device with your credentials. • Key Based - Unverified—The new fingerprint on the device is not updated in the Junos Space Platform database. • Key Conflict - Unverified—The key upload was unsuccessful; the new fingerprint on the device is not updated in the Junos Space Platform database. • Credentials Based - Unverified—The new fingerprint on the device is not updated in the Junos Space Platform database. • Key Conflict—The device was not available; the key upload was unsuccessful. • Fingerprint Conflict—The fingerprint stored in the Junos Space Platform database differs from the fingerprint on the device. • NA—The device is unmanaged.
Aggregation Device	Mode of the aggregation device: single-home or multihome
Satellite Devices(Number)	Number of satellite devices connected to the aggregation device

Table 18: Fields in the Device Management Table *(continued)*

Field	Description
Connection Type	• Reachable Device initiated—This is a device-initiated connection from an internal device (without a NAT server to route the connection) and the device is reachable. • Reachable Device initiated–External—This is a device-initiated connection from an external device (NAT server routes the connection) and the device is reachable. • Junos Space initiated—This is a connection initiated by Junos Space to an internal device (without a NAT server to route the connection). • Junos Space initiated–External—This is a connection initiated by Junos Space to an external device (NAT server routes the connection) and the device is reachable. • Modeled—This is a device-initiated connection and the device is unreachable.
Device Network	Whether the device is connected to Junos Space Platform through a NAT server • Internal—The device is connected to Junos Space Platform directly—that is, without a NAT server • External—The NAT server routes the connection to Junos Space Platfom

2. (Optional) Sort the table by mousing over the column head for the data that you want to sort and clicking the down arrow. Select **Sort Ascending** or **Sort Descending**.

3. (Optional) Show columns not in the default tabular view, or hide columns, as follows:

   a. Mouse over any column head and click the down arrow.

   b. Select **Columns** from the menu.

   c. Select the check boxes against the columns that you want to view. Clear the check boxes against the columns that you want to hide.

4. (Optional) View information about devices as follows:

   - To restrict the display of devices, enter search criteria of one or more characters in the Search field and press Enter.

     All devices that match the search criteria are shown in the main display area.

   - To view hardware inventory for a device, select the row against the device and select **Device Inventory > View Physical Inventory** from the Actions menu. Alternatively, right-click the device name and select **Device Inventory > View Physical Inventory**.

   - To view the physical or logical interfaces of a device, click the **View** link in the appropriate column and row for the device.

     To view the physical or logical interfaces of more than one device, select the required devices, right-click and select **Device Inventory > View Logical Interfaces**.

The View Logical Interfaces page displays the list of logical interfaces of the selected devices.

Release History Table

Release	Description
16.1R1	Reachable Device initiated–External—This is a device-initiated connection from an external device (NAT server routes the connection) and the device is reachable.
16.1R1	Junos Space initiated–External—This is a connection initiated by Junos Space to an external device (NAT server routes the connection) and the device is reachable.

RELATED DOCUMENTATION

- Viewing the Physical Inventory | 301
- Exporting the License Inventory | 312
- Viewing Physical Interfaces of Devices | 306
- Device Discovery Profiles Overview | 220
- Viewing the Node List | 809
- Resynchronizing Nodes in Network Monitoring | 813
- Systems of Record in Junos Space Overview | 214

Juniper Networks Devices Supported by Junos Space Network Management Platform

Table 19 lists all the Juniper Networks product series and devices supported by Junos Space Network Management Platform. The Junos Space Platform release notes lists only the new devices that are supported with that release.

NOTE: Ensure that you install the exact matching or closest matching of Junos OS schema on the Junos Space Platform. For more information, see Table 20.

Table 19: Devices Supported by Junos Space Platform

Product Series	Model	Junos Space Release
ACX Series	ACX500	Junos Space Platform 14.1R2 or later
	ACX710	Junos Space 20.1R1 hot patch v1 or later
	ACX1000	Junos Space Platform 12.2 or later
	ACX1100	Junos Space Platform 12.3 or later
	ACX2000	Junos Space Platform 12.2 or later
	ACX2100	Junos Space Platform 12.3 or later
	ACX2200	Junos Space Platform 12.3 or later
	ACX4000	Junos Space Platform 13.1 or later
	ACX5048	Junos Space Platform 15.1 or later
	ACX5096	Junos Space Platform 15.1 or later
	ACX5448	Junos Space Platform 18.4 or later
BX Series	BX7000	Junos Space Platform 11.3 or later

Table 19: Devices Supported by Junos Space Platform *(continued)*

Product Series	Model	Junos Space Release
EX Series	EX2200	Junos Space Platform 16.1 or later
	EX2300	Junos Space Platform 15.2R2 or later
	EX2300-24MP	Junos Space Platform 18.1 or later
	EX2300-48MP	Junos Space Platform 17.2 or later
	EX3300	Junos Space Platform 11.4 or later
	EX3400	Junos Space Platform 15.2R2 or later
	EX4300	Junos Space Platform 13.1 or later
	EX4300-48MP	Junos Space Platform 18.3R1 or later
	EX4500	Junos Space Platform 12.2 or later
	EX4550	Junos Space Platform 12.2 or later
	EX4550-40G	Junos Space Platform 12.2 or later
	EX4600	Junos Space Platform 13.3 or later
	EX4650	Junos Space Platform 18.4 or later
	EX6200	Junos Space Platform 13.2 or later
	EX6210	Junos Space Platform 11.4 or later
	EX9200	Junos Space Platform 13.1 or later
	EX9204	Junos Space Platform 13.1 or later
	EX9208	Junos Space Platform 13.1 or later
	EX9214	Junos Space Platform 13.1 or later
	EX9251	Junos Space Platform 18.1 or later
	EX9253	Junos Space Platform 18.2 or later

Table 19: Devices Supported by Junos Space Platform *(continued)*

Product Series	Model	Junos Space Release
EX Virtual Chassis	EX2200-VC	Junos Space Platform 18.4 or later
	EX2300-VC	Junos Space Platform 18.4 or later
	EX3300-VC	Junos Space Platform 15.2 or later
	EX4200-VC	Junos Space Platform 11.4 or later
	EX4300-VC	Junos Space Platform 13.1 or later
	EX4550-VC	Junos Space Platform 13.1 or later
	EX4600-VC	Junos Space Platform 16.1 or later
	EX-XRE	Junos Space Platform 14.1R2 or later
Firefly	vSRX Firefly	Junos Space Platform 15.1 or later
Junos Fusion	Junos Fusion Edge	Junos Space Platform 17.1 or later
LN Series	LN1000	Junos Space Platform 12.3 or later
	LN2600	Junos Space Platform 12.3 or later
M Series	M7i M10i M40e M120 M320	Junos Space Platform 16.1 or later
MCG Series	MCG5000	Junos Space Platform 11.3 or later

Table 19: Devices Supported by Junos Space Platform *(continued)*

Product Series	Model	Junos Space Release
MX Series	MX5	Junos Space Platform 12.1 or later
	MX10	Junos Space Platform 11.4 or later
	MX80	Junos Space Platform 14.1 or later
	MX104	Junos Space Platform 13.2 or later
	MX204	Junos Space Platform 18.2 or later
	MX240	Junos Space Platform 13.1 or later
	MX480	Junos Space Platform 13.1 or later
	MX960	Junos Space Platform 13.1 or later
	MX10003	Junos Space Platform 18.4 or later
	MX10008	Junos Space Platform 18.4 or later
	MX10016	Junos Space Platform 18.4 or later
	MX2008	Junos Space Platform 17.1 or later
	MX2010	Junos Space Platform 12.3 or later
	MX2020	Junos Space Platform 12.3 or later
MX Series Virtual Chassis	MX-VC	Junos Space Platform 14.1 or later
PTX Series	PTX1000	Junos Space Platform 17.1 or later
	PTX3000	Junos Space Platform 13.2 or later
	PTX5000	Junos Space Platform 12.3 or later
	PTX10008	Junos Space Platform 17.2 or later
	PTX10016	Junos Space Platform 17.2 or later
	PTX10001-20C	Junos Space Platform 18.3R1 or later

Table 19: Devices Supported by Junos Space Platform *(continued)*

Product Series	Model	Junos Space Release
QFX Series	QFX3000	Junos Space Platform 12.2 or later
	QFX3000-G	Junos Space Platform 12.2 or later
	QFX3000-M	Junos Space Platform 12.2 or later
	QFX3500	Junos Space Platform 12.3 or later
	QFX3600	Junos Space Platform 13.1 or later
	QFX5100	Junos Space Platform 13.2 or later
	QFX5110-32Q	Junos Space Platform 17.1 or later
	QFX5110-48S	Junos Space Platform 17.1 or later
	QFX5120-32C	Junos Space Platform 19.4 or later
	QFX5120	Junos Space Platform 18.4 or later
	QFX5210	Junos Space Platform 18.4 or later
	QFX5200	Junos Space Platform 15.1R2 or later
	QFX5200-48Y	Junos Space Platform 18.1 or later
	QFX5210-64C	Junos Space Platform 18.1 or later
	QFX10002-36Q	Junos Space Platform 15.1 or later
	QFX10002-36Q-DC	Junos Space Platform 15.1 or later
	QFX10002-60C	Junos Space Platform 18.1 or later
	QFX10002-72Q	Junos Space Platform 15.1 or later
	QFX10002-72Q-DC	Junos Space Platform 15.1 or later
	QFX10008	Junos Space Platform 15.1R2 or later
	QFX10016	Junos Space Platform 15.1R2 or later

Table 19: Devices Supported by Junos Space Platform *(continued)*

Product Series	Model	Junos Space Release
QFX Series Virtual Chassis	QFX-VC	Junos Space Platform 14.1 or later

Table 19: Devices Supported by Junos Space Platform *(continued)*

Product Series	Model	Junos Space Release
SRX Series	SRX100	Junos Space Platform 11.4 or later
	SRX110H-VB	Junos Space Platform 13.1 or later
	SRX210	Junos Space Platform 13.1 or later
	SRX220	Junos Space Platform 13.1 or later
	SRX240	Junos Space Platform 13.1 or later
	SRX240H	Junos Space Platform 14.1R1 or later
	SRX300	Junos Space Platform 15.1R2 or later
	SRX320	Junos Space Platform 15.1R2 or later
	SRX320-PoE	Junos Space Platform 15.1R2 or later
	SRX340	Junos Space Platform 15.1R2 or later
	SRX345	Junos Space Platform 15.1R2 or later
	SRX380	Junos Space 20.1R1 hot patch v1 or later
	SRX550	Junos Space Platform 15.1R2 or later
	SRX550-M	Junos Space Platform 15.1R2 or later
	SRX650	Junos Space Platform 13.1 or later
	SRX1400	Junos Space Platform 16.1 or later
	SRX1500	Junos Space Platform 15.1R2 or later
	SRX3400	Junos Space Platform 14.1R1 or later
	SRX4100	Junos Space Platform 16.1 or later
	SRX4200	Junos Space Platform 16.1 or later

Table 19: Devices Supported by Junos Space Platform *(continued)*

Product Series	Model	Junos Space Release
	SRX4600	Junos Space Platform 17.2 or later
	SRX5400	Junos Space Platform 13.2 or later
	SRX5600	Junos Space Platform 18.2 or later
	SRX5800	Junos Space Platform 13.3 or later
	SRX3600	Junos Space Platform 13.3 or later
Virtual SRX Series	vSRX 3.0	Junos Space Platform 18.2 or later
T Series	T4000	Junos Space Platform 12.2 or later
Virtual MX Series	vMX	Junos Space Platform 15.1 or later
Virtual route reflector (VRR)	VRR	Junos Space Platform 14.1R2 or later
WLC Series	WLC device	Junos Space Platform 14.1 or later

Table 20: Devices Supported by Junos Space Platform with Compatible Junos OS Releases

Product Series	Model	Supported Junos Operating System (Junos OS) Releases	Qualified Schema Version
ACX Series	ACX710	20.2R1	20.2R1
	ACX5448	18.3R1 18.4R1.8 or later	18.4R1.8 18.4R1.8

Table 20: Devices Supported by Junos Space Platform with Compatible Junos OS Releases *(continued)*

Product Series	Model	Supported Junos Operating System (Junos OS) Releases	Qualified Schema Version
EX Series	EX2200	12.3R12-S10 14.1X53-D44.3 or later	12.3R12-S10 14.1X53-D44.3
	EX2300	18.1R3.3 18.4R1.8 or later	18.1R3.3 18.4R1.8
	EX3300	12.3R12-S10 15.1R7.9 or later	12.3R12-S10 15.1R7.9
	EX3400	18.1R3.3 18.4R1.8 or later	18.1R3.3 18.4R1.8
	EX4300	17.3R3-S1.5 18.4R1.8 or later	17.3R3-S1.5 18.4R1.8
	EX4300-48MP	17.3R3-S1.5 18.4R1.8 or later	- 18.4R1.8
	EX4500	15.1R7.9 or later	15.1R7.9
	EX4550	15.1R7.9 or later	15.1R7.9
	EX4600	17.3R3-S1.5 18.4R1.8 or later	17.3R3-S1.5 18.4R1.8
	EX4650	18.4R1.8 or later	18.4R1.8
	EX9200	17.3R3-S1.5 18.3R1.9 or later	17.3R3-S1.5 18.3R1.9

Table 20: Devices Supported by Junos Space Platform with Compatible Junos OS Releases *(continued)*

Product Series	Model	Supported Junos Operating System (Junos OS) Releases	Qualified Schema Version
EX Virtual Chassis	EX2200-VC	12.3R12-S12	12.3R1.7
	EX2300-VC	18.2R1.9	12.3R1.7
	EX4200-VC	12.2R1 or later	15.1R7.9
MX Series	MX204	18.4R1 or later	18.4R1.8
	MX240	13.2R2.4 or later	17.3R3.9 18.4R1.8
	MX480	13.2R2.4 or later	17.3R3-S2.2 17.3R3.9 19.1R1.6
	MX10003	18.4R1.8 or later	18.4R1.8
	MX10008	18.4R1.8 or later	18.4R1.8
	MX10016	18.4R1.8 or later	18.4R1.8

Table 20: Devices Supported by Junos Space Platform with Compatible Junos OS Releases *(continued)*

Product Series	Model	Supported Junos Operating System (Junos OS) Releases	Qualified Schema Version
QFX Series	QFX5100	17.3R3 or later	17.3R3-S1.5 18.4R1.8
	QFX5110-32Q	17.3R3 or later	17.3R3-S1.5 19.1R1.6
	QFX5110-48S	17.3R3-S1.5 19.1R1.6 or later	17.3R3-S1.5 19.1R1.6
	QFX5120	18.4R1.8 or later	18.4R1.8
	QFX5210	19.1R1.6 or later	19.1R1.6
	QFX5200	17.3R3 or later	17.3R3.9 18.4R1.8
	QFX10002-36Q	17.3R3 or later	17.3R3-S1.5 19.1R1.6
	QFX10002-36Q-DC	17.3R3 or later	17.3R3-S1.5 19.1R1.6
	QFX10002-60C	17.3R3 or later	17.3R3-S1.5 19.1R1.6
	QFX10002-72Q	17.3R3 or later	17.3R3-S1.5 19.1R1.6
	QFX10002-72Q-DC	17.3R3-S1.5 or later	17.3R3-S1.5
	QFX10008	17.3R3 or later	17.3R3.9 18.4R1.8
SRX Series	SRX380	20.2R1	20.2R1

RELATED DOCUMENTATION

Device Management Overview | 189

Viewing Managed Devices | 194

Device Discovery Profiles Overview | 220

Junos OS Releases Supported in Junos Space Network Management Platform | 334

Uploading Device Tags by Using a CSV File

Device tags help you easily identify managed devices when deploying a device template, upgrading a device image, staging scripts, or applying CLI Configlets to devices. Device tags associate the IP address or hostname of a managed device with a tag.

Starting with Junos Space Network Management Platform Release 15.2R1, you can upload device tags from the local computer to Junos Space Network Management Platform. You use the Devices workspace to upload device tags by using a CSV file. You can assign the tags created using this task to other Junos Space objects. For more information, refer to "Tagging an Object" on page 1526.

> **NOTE:** You must create a CSV file with the correct IP address or hostname of a device, tag name, and tag type, which could be private or public. If you do not specify whether the tag is private or public, by default a public tag is created.
>
> Tag names must not exceed 255 characters. Tag names must not start with a space, and cannot contain a comma, double quotation marks, and parentheses. Also, you cannot name a tag "Untagged" because it is a reserved term.
>
> Entries pertaining to incorrect IP addresses or hostnames are not uploaded to Junos Space Platform. You can view incorrect entries in the job results.

To upload device tags by using a CSV file:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page that appears displays all devices managed by Junos Space Platform.

2. Click the Tag Devices by CSV icon.

   The Upload Tags CSV File pop-up window is displayed.

3. (Optional) To view a sample CSV file, click the **Sample CSV** hyperlink.

4. Click **Browse** to select the CSV file from the local computer.

5. Click **Import**.

   The details of the devices and tags are uploaded to Junos Space Platform. A Job Information dialog box is displayed.

   a. Click **OK**.

      You are redirected to the Device Management page.

   To view job details:

   a. Click the job ID in the Job Information dialog box.

      You are redirected to the Job Management page with the filtered view of the job.

When the job is complete, all devices with correct details are assigned the tags you uploaded through the CSV file. To view the tags, go to **Administration > Tags**.

Release History Table

Release	Description
15.2R1	Starting with Junos Space Network Management Platform Release 15.2R1, you can upload device tags from the local computer to Junos Space Network Management Platform.

RELATED DOCUMENTATION

Tags Overview | **1506**

Deleting Tags | **1523**

Exporting Tags from Junos Space Network Management Platform | **1533**

Filtering Devices by CSV

You can filter the devices on the Device Management page using a CSV file.

To filter devices using a CSV file:

1. On the Junos Space Network Management Platform user interface, select **Devices >Device Management.**

   The Device Management page is displayed.

2. Select **Filter by CSV** from the Actions menu.

   The Select CSV File pop-up window is displayed.

3. (Optional) To view a sample CSV file, click the **Sample CSV** hyperlink.

4. Click **Browse** and select the CSV file from the local computer.

5. Click **Import**.

   A progress bar is displayed. Junos Space Network Management Platform validates the values you provided in the CSV file. If the validation fails, a pop-window is displayed. This pop-up window displays the list of devices that were not validated.

   If the CSV file is imported successfully, the Device Management page is filtered and lists only those devices whose host names were listed in the CSV file.

RELATED DOCUMENTATION

Device Management Overview | 189

Uploading Device Tags by Using a CSV File | 211

CHAPTER 8

Systems of Record

IN THIS CHAPTER

- Systems of Record in Junos Space Overview | 214
- Understanding How Junos Space Automatically Resynchronizes Managed Devices | 216

Systems of Record in Junos Space Overview

IN THIS SECTION

- Systems of Record | 214
- Implications on device management | 215

Although by default the Junos Space network you are administering is the system of record (SOR)—each device defines its own official state—you may prefer to have the Junos Space Network Management Platform database contain the official state of the network, enabling you to restore that official state if unwanted out-of-band changes are made to a device. This feature enables you to designate Junos Space Network Management Platform as the SOR if you prefer.

Systems of Record

A network managed by Junos Space Network Management Platform contains two repositories of information about the devices in the network: the devices themselves (each device defines and reports its official state) and the Junos Space Network Management Platform database (which contains information that is reported by the device during device discovery). One of these repositories must have precedence over the other as the accepted desirable state. By default, the network itself is the system of record (NSOR).

In NSOR, when a local user commits a change in the configuration of a network device, the commit operation triggers a report via system log to Junos Space Network Management Platform. The values in the Junos

Space Network Management Platform database are automatically changed to match the new device values, and the timestamps are synchronized. Thus the devices control the contents of the database.

As of version 12.2, you can designate the Junos Space Network Management Platform database values as having precedence over any values configured locally at a device. In this scenario, Junos Space Network Management Platform (database) is the system of record (SSOR). It contains the configurations that the Junos Space administrator considers best for the network devices. If an out-of-band commit operation is executed on a network device, Junos Space Network Management Platform receives a system log message, but the values in the Junos Space Network Management Platform database are not automatically changed or synchronized. Instead, the administrator can choose whether or not to overwrite the device's local changes by pushing the accepted configuration to the device from the Junos Space Network Management Platform database.

The choice of pushing the Junos Space Network Management Platform configuration is left to the administrator because the local device changes may, for example, be part of a temporary test that the administrator would not want to interrupt. However, if the tester forgets to reset the configuration at the end of the test, the administrator might then push the SSOR configuration to the device.

Implications on device management

The basic difference between NSOR and SSOR lies in whether or not the Junos Space Network Management Platform database is automatically synchronized when changes are made to a network device, and which set of values has precedence.

Setting the Junos Space Network Management Platform database as the system of record does not protect your network from local changes. The device notifies Junos Space Network Management Platform via system log when the changes occur, and it does not resynchronize, so you still have the previous configuration and you can reset the remote device quickly if you need to do so. In an NSOR scenario, Junos Space Network Management Platform is also notified via system log. You can still push a more desirable configuration to the device, but this process is less efficient.

In the NSOR scenario, you can disable automatic resynchronization. When autoresynchronozation is turned off, the server continues to receive notifications and goes into the out-of-sync state; however, autoresynchronozation does not run on the device. You can manually resynchronize a device in such a case.

NSOR with automatic resynchronization disabled is not equivalent to SSOR: manually resynchronizing under NSOR updates the values in the Junos Space Network Management Platform database to reflect those on the device. This never happens under SSOR, where the Junos Space Network Management Platform database values have precedence over the device values, and synchronizing them involves pushing the database values to the device, effectively resetting the device’s out-of-band changes.

RELATED DOCUMENTATION

Understanding How Junos Space Automatically Resynchronizes Managed Devices

IN THIS SECTION

- Network as System of Record | 216
- Junos Space as System of Record | 218

When configuration changes are made on a physical device that Junos Space Network Management Platform manages, Junos Space Platform reacts differently depending on whether the network itself is the system of record (NSOR) or Junos Space Platform is the system of record (SSOR).

In the NSOR case, Junos Space Platform receives a system log message from the modified device and automatically resynchronizes the configuration values in its database with those of the device. This ensures that the device inventory information in the Junos Space Platform database matches the current configuration information on the device.

In the SSOR case, the Junos Space Platform receives a system log message from the modified device. The Managed Status of that device changes from In Sync to Device Changed (if the changes are made from the device CLI), Space Changed (if the changes are made from Junos Space Platform), or Space & Device Changed (if the changes are made both from the device CLI and Junos Space Platform), but no resynchronization occurs. The Junos Space Platform administrator can choose whether or not to reset the device's configuration to match the configuration values in the Junos Space Platform database.

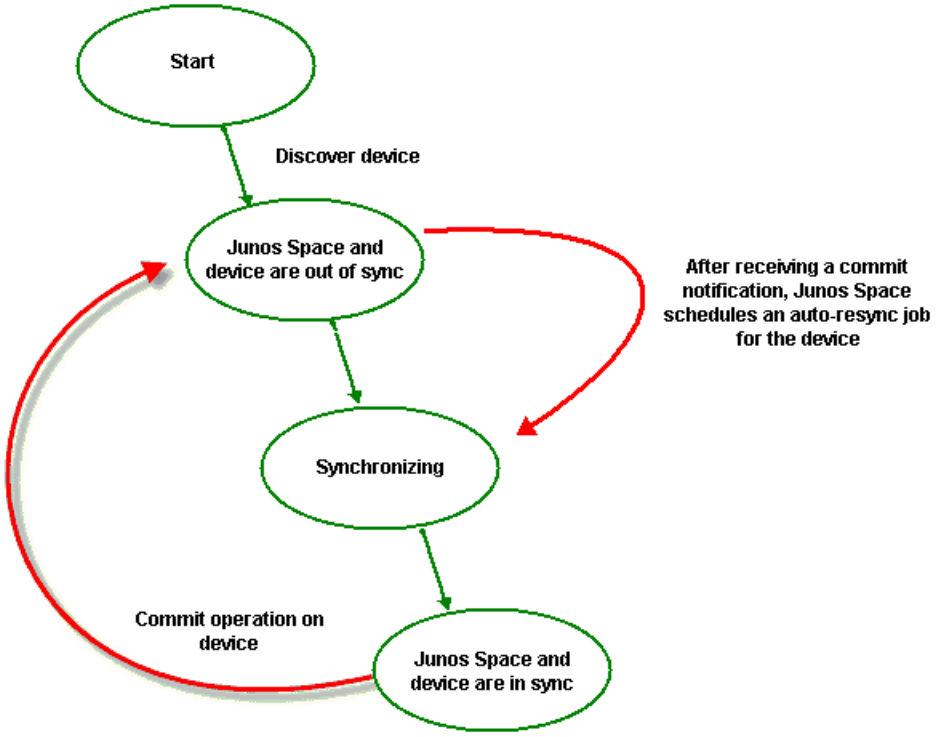
This topic covers:

Network as System of Record

After Junos Space Platform discovers and imports a device, if the network is the system of record, Junos Space Platform enables the auto-resynchronization feature on the device by initiating a commit operation.

After auto-resynchronization is enabled, any configuration changes made on the device, including out-of-band CLI commits and change-request updates, automatically trigger resynchronization on the device. Figure 46 shows how a commit operation resynchronizes the configuration information in the Junos Space Platform database with that on the device.

Figure 46: Resynchronization Process



When a commit operation is performed on a managed device in NSOR mode, Junos Space Platform, by default, schedules a resynchronization job to run 20 seconds after the commit operation is received. However, if Junos Space Platform receives another commit notification within 20 seconds of the previous commit notification, no additional resynchronization jobs are scheduled because Junos Space Platform resynchronizes both commit operations in one job. This damping feature of automatic resynchronization provides a window of time during which multiple commit operations can be executed on the device, but only one or a few resynchronization jobs are required to resynchronize the Junos Space Platform database with the multiple configuration changes executed on the device.

You can change the default value of 20 seconds to any other duration by specifying the value in seconds in the **Administration > Applications > Network Management Platform > Modify Application Settings > Device > Max auto resync waiting time secs** field. For example, if you set the value of this field to 120 seconds, then Junos Space Platform automatically schedules a resynchronization job to run 120 seconds after the first commit operation is received. If Junos Space Platform receives any other commit notification within these 120 seconds, it resynchronizes both commit operations in one job.

For information about setting the damper interval to change the resynchronization time delay and information about disabling the auto-resynchronization feature, see “Modifying Settings of Junos Space Applications” on page 1345.

When Junos Space Platform receives the device commit notification, the Managed Status is Out of Sync. When the resynchronization job begins on the device, the Managed Status of the device changes to Synchronizing and then In Sync after the resynchronization job has completed, unless a pending device commit operation causes the device to display Out of Sync while it was synchronizing.

When a resynchronization job is scheduled to run but another resynchronization job on the same device is in progress, Junos Space Platform delays the scheduled resynchronization job. The time delay is determined by the damper interval that you can set from the Application workspace. By default, the time delay is 20 seconds. The scheduled job is delayed as long as the other resynchronization job to the same device is in progress. When the currently running job finishes, the scheduled resynchronization job starts.

You can disable the auto-resynchronization feature in the Administration workspace. When auto-resynchronization is turned off, the server continues to receive notifications and goes into the Out of Sync state; however, the auto-resynchronization feature does not run on the device. To resynchronize a device when the auto-resynchronization feature is disabled, use the Resynchronize with Network workflow. The auto-resynchronization jobs are not displayed on the Job Management page. These jobs run in the background and cannot be canceled from the Junos Space user interface. You can view the status of the auto-resynchronization job in the Managed Status column on the Device Management page or from the Device Count by Synchronization State widget on the Devices page. You can collect more information about these jobs from the **server.log** and **autoresync.log** files in the **/var/log/jboss/servers/server1** directory.

> **NOTE:** You can view the auto-resynchronization jobs that were scheduled to execute before upgrading to Junos Space Platform Release 15.1R1, from the Job Management page.

Junos Space as System of Record

If Junos Space Platform is the system of record, automatic resynchronization of the configuration information between the Junos Space Platform database and the managed device does not occur. When Junos Space Platform receives a system log message from the modified device, the Managed Status of the device goes from In Sync to Device Changed (if the changes are made from the device CLI), Space Changed (if the changes are made from Junos Space Platform), or Space & Device Changed (if the changes are made both from the device CLI and Junos Space Platform) and remains so unless you manually push the system of record configuration from the Junos Space Platform database to the device.

RELATED DOCUMENTATION

Systems of Record in Junos Space Overview | 214

Device Discovery Profiles Overview | 220

Device Inventory Overview | 299

Resynchronizing Managed Devices with the Network | 448

CHAPTER 9

Device Discovery Profiles

IN THIS CHAPTER

- Device Discovery Profiles Overview | 220
- Creating a Device Discovery Profile | 226
- Running Device Discovery Profiles | 238
- Modifying a Device Discovery Profile | 239
- Cloning a Device Discovery Profile | 241
- Viewing a Device Discovery Profile | 243
- Deleting Device Discovery Profiles | 244
- Exporting the Device Discovery Details As a CSV File | 245

Device Discovery Profiles Overview

IN THIS SECTION

- Connections Initiated by Junos Space or the Device | 221
- Device Information Fetched During Device Discovery | 225

You use the device discovery profile to add devices to Junos Space Network Management Platform from the Devices workspace. *Discovery* is the process of finding a device and then synchronizing the device inventory and configuration with the Junos Space Network Management Platform database. To use device discovery, you must be able to connect Junos Space Network Management Platform to the device.

A device discovery profile contains preferences used to discover devices, such as discovery targets, probes used to discover devices, mode and details for authentication, SSH fingerprints of devices, and the schedule to use this discovery profile. You can start the discovery process using a discovery profile in the following ways: scheduling a discovery after creating a discovery profile, or selecting a discovery profile and clicking Run Now.

Executing or running a discovery profile discovers, authenticates, and manages the device on Junos Space Network Management Platform. With appropriate privileges for discovering devices, you can create multiple discovery profiles with different combinations of targets, probes, and authentication modes on your Junos Space setup. You can clone, modify, and delete the device discovery profiles from Junos Space Network Management Platform. You can also choose whether to share device discovery profiles with other users with device discovery permissions.

To discover network devices using a device discovery profile, Junos Space Network Management Platform uses the SSH, ICMP Ping, and SNMP protocols. When the device is discovered, device authentication is handled through the administrator login SSH v2 credentials and SNMP v1, SNMP v2c, or SNMP v3 settings, keys generated from Junos Space Network Management Platform (RSA, DSS, or ECDSA keys), or custom keys. You can optionally enter the SSH fingerprint for each device and let Junos Space Network Management Platform save the fingerprint in the database during the discovery process and validate the fingerprint when the device connects to Junos Space Network Management Platform. Fingerprint validation is available only for SSH-enabled Juniper Networks devices and not for ww Junos OS devices and modeled devices. For more information about device authentication in Junos Space, see “Device Authentication in Junos Space Overview” on page 281.

For device targets, you can specify a single IP address, a DNS hostname, an IP range, or an IP subnet to discover devices on a network. When a device discovery profile is executed or run (either instantly or based on a schedule), Junos Space Network Management Platform connects to the physical device and retrieves the running configuration and the status information of the device. To connect with and configure devices, Junos Space Network Management Platform uses the Device Management Interface (DMI) of Juniper Networks devices, which is an extension of the NETCONF network configuration protocol.

Connections Initiated by Junos Space or the Device

When a device is discovered , Junos Space Network Management Platform creates an object in the Junos Space Network Management Platform database to represent the physical device and maintains a connection between the object and the physical device so that their information is linked.

Junos Space can manage devices in either of the following ways:

- Junos Space initiates and maintains a connection to the device.

- The device initiates and maintains a connection to Junos Space.

By default, Junos Space manages devices by initiating and maintaining a connection to the device. When Junos Space initiates the connection to the device, you can discover and manage devices irrespective of whether the management system is behind a Network Address Translation (NAT) server. For ww Junos OS devices, Junos Space uses SSH with an adapter to manage the devices.

For Junos Space-initiated connection, it configures the following Junos OS CLI commands on the device during device discovery:

Standalone SRX Series Devices

```
set system services ssh max-sessions-per-connection 32
set system syslog file default-log-messages any info
set system syslog file default-log-messages match "(requested 'commit'
operation)|(copying configuration to juniper.save)|(commit
complete)|ifAdminStatus|(FRU power)|(FRU removal)|(FRU insertion)|(link
UP)|transitioned|Transferred|transfer-file|(license add)|(license
delete)|(package -X update)|(package -X delete)|(FRU Online)|(FRU
Offline)|(plugged in)|(unplugged)|GRES|(AIS_DATA_AVAILABLE)"
set system syslog file default-log-messages structured-data
set snmp trap-group space targets <space-ip-address>
```

Cluster SRX

```
set groups node0 system services ssh max-sessions-per-connection 32
set groups node0 system syslog file default-log-messages any info
set groups node0 system syslog file default-log-messages match "(requested
'commit' operation)|(copying configuration to juniper.save)|(commit
complete)|ifAdminStatus|(FRU power)|(FRU removal)|(FRU insertion)|(link
UP)|transitioned|Transferred|transfer-file|(license add)|(license
delete)|(package -X update)|(package -X delete)|(FRU Online)|(FRU
Offline)|(plugged in)|(unplugged)|GRES|(AIS_DATA_AVAILABLE)"
set groups node0 system syslog file default-log-messages structured-data
set groups node1 system services ssh max-sessions-per-connection 32
set groups node1 system syslog file default-log-messages any info
set groups node1 system syslog file default-log-messages match "(requested
'commit' operation)|(copying configuration to juniper.save)|(commit
complete)|ifAdminStatus|(FRU power)|(FRU removal)|(FRU insertion)|(link
UP)|transitioned|Transferred|transfer-file|(license add)|(license
```

```
delete)|(package -X update)|(package -X delete)|(FRU Online)|(FRU
Offline)|(plugged in)|(unplugged)|GRES|(AIS_DATA_AVAILABLE)"
set groups node1 system syslog file default-log-messages structured-data
set snmp trap-group space targets <space-ip-address>
```

EX Series

```
set system services ssh max-sessions-per-connection 32
set system syslog file default-log-messages any any
set system syslog file default-log-messages match "(requested 'commit'
operation)|(copying configuration to juniper.save)|(commit
complete)|ifAdminStatus|(FRU power)|(FRU removal)|(FRU insertion)|(link
UP)|transitioned|Transferred|transfer-file|(license add)|(license
delete)|(package -X update)|(package -X delete)|(FRU Online)|(FRU
Offline)|(plugged in)|(unplugged)|cm_device|(Master Unchanged, Members
Changed)|(Master Changed, Members Changed)|(Master Detected, Members
Changed)|(vc add)|(vc delete)|(Master detected)|(Master changed)|(Backup
detected)|(Backup changed)|(interface vcp-)|(AIS_DATA_AVAILABLE)"
set system syslog file default-log-messages structured-data
set snmp trap-group space targets <space-ip-address>
```

QFX Series

```
set system services ssh max-sessions-per-connection 32
set system syslog file default-log-messages any any
set system syslog file default-log-messages match "(requested 'commit'
operation)|(copying configuration to juniper.save)|(commit
complete)|ifAdminStatus|(FRU power)|(FRU removal)|(FRU insertion)|(link
UP)|transitioned|Transferred|transfer-file|(license add)|(license
delete)|(package -X update)|(package -X delete)|(FRU Online)|(FRU
Offline)|(plugged
in)|(unplugged)|QF_NODE|QF_SERVER_NODE_GROUP|QF_INTERCONNECT|QF_DIRECTOR|QF_NETWORK_NODE_GROUP|(Master
 Unchanged, Members Changed)|(Master Changed, Members Changed)|(Master
Detected, Members Changed)|(vc add)|(vc delete)|(Master detected)|(Master
changed)|(Backup detected)|(Backup changed)|(interface
vcp-)|(AIS_DATA_AVAILABLE)"
set system syslog file default-log-messages structured-data
```

```
set snmp trap-group space targets <space-ip-address>
```

MX Series

```
set system services ssh max-sessions-per-connection 32
set system syslog file default-log-messages any info
set system syslog file default-log-messages match "(requested 'commit'
operation)|(copying configuration to juniper.save)|(commit
complete)|ifAdminStatus|(FRU power)|(FRU removal)|(FRU insertion)|(link
UP)|transitioned|Transferred|transfer-file|(license add)|(license
delete)|(package -X update)|(package -X delete)|(FRU Online)|(FRU
Offline)|(plugged in)|(unplugged)|CFMD_CCM_DEFECT| LFMD_3AH |
RPD_MPLS_PATH_BFD|(Master Unchanged, Members Changed)|(Master Changed, Members
 Changed)|(Master Detected, Members Changed)|(vc add)|(vc delete)|(Master
detected)|(Master changed)|(Backup detected)|(Backup changed)|(interface
vcp-)|(AIS_DATA_AVAILABLE)"
set system syslog file default-log-messages structured-data
set snmp trap-group space targets <space-ip-address>
```

If a device-initiated connection to Junos Space is enabled, the DMI channel and port 7804 are used and the following (sample) configuration is added on the device to establish the connection to Junos Space:

```
set system services outbound-ssh client 00111DOCEFAC device-id 7CE5FE
set system services outbound-ssh client 00111DOCEFAC secret “$ABC123”
set system services outbound-ssh client 00111DOCEFAC services netconf
set system services outbound-ssh client 00111DOCEFAC  172.22.199.10 port 7804
```

To discover and manage devices through a device-initiated connection, clear the **Junos Space initiated connection to device** check box on the Modify Application Settings page in the Administration workspace. For information about configuring connections initiated by Junos Space by a device, see “Modifying Junos Space Network Management Platform Settings” on page 1346.

You can configure a NAT server to route connections between the Junos Space setup and managed devices. Both device-initiated connections to a Junos Space setup and connections initiated by Junos Space to managed devices, when the Junos Space setup is behind the NAT server, are supported on Junos Space Network Management Platform. If a NAT server is used, the managed devices connect to Junos Space Network Management Platform through the IP address of Junos Space Network Management Platform translated by NAT. For more information about using a NAT server on a Junos Space setup, see “NAT Configuration for Junos Space Network Management Platform Overview” on page 1288.

When configuration changes are made in Junos Space Network Management Platform—for example, when you deploy service orders to activate a service on your network devices—the configuration is pushed to the physical device.

If the network is the system of record (NSOR), when configuration changes are made on the physical device (out-of-band CLI commits and change-request updates), Junos Space Network Management Platform automatically resynchronizes with the device so that the device inventory information in the Junos Space Network Management Platform database matches the current device inventory and configuration information. If Junos Space Network Management Platform is the system of record (SSOR), this resynchronization does not occur and the database is unchanged.

Device Information Fetched During Device Discovery

The following device inventory and configuration data are captured and stored in relational tables in the Junos Space Network Management Platform database:

- Devices—Hostname, IP address, credentials
- Physical Inventory—Chassis, FPM board, power entry module (PEM), Routing Engine, Control Board (CB), Flexible PIC Concentrator (FPC), CPU, PIC, transceiver, fan tray

  Junos Space Network Management Platform displays the model number, part number, serial number, and description for each inventory component, when applicable.
- Logical Inventory—Subinterfaces, encapsulation (link-level), type, speed, maximum transmission unit (MTU), VLAN ID
- License information:
  - License usage summary—License feature name, feature description, licensed count, used count, given count, needed count
  - Licensed feature information—Original time allowed, time remaining
  - License SKU information—Start date, end date, and time remaining
- Loopback interface

Other device configuration data is stored in the Junos Space Network Management Platform database as binary large objects and is available only to northbound interface (NBI) users.

Release History Table

Release	Description
16.1R1	You use the device discovery profile to add devices to Junos Space Network Management Platform from the Devices workspace.

RELATED DOCUMENTATION

Creating a Device Discovery Profile | 226
Running Device Discovery Profiles | 238
Cloning a Device Discovery Profile | 241
Viewing a Device Discovery Profile | 243
Viewing Managed Devices | 194
Systems of Record in Junos Space Overview | 214
Understanding How Junos Space Automatically Resynchronizes Managed Devices | 216
Resynchronizing Managed Devices with the Network | 448
Device Management Overview | 189
Device Inventory Overview | 299
DMI Schema Management Overview | 1534

Creating a Device Discovery Profile

You create a device discovery profile to create a set of preferences for device targets, probes, authentication mode and credentials, SSH fingerprints, and the schedule to discover devices to Junos Space Network Management Platform. In addition to scheduling the discovery, you can manually start the discovery process by running the device discovery profile. For more information, see “Running Device Discovery Profiles” on page 238.

NOTE: To discover a device with dual Routing Engines, always specify the IP address of the current primary Routing Engine. When the current primary IP address is specified, Junos Space Network Management Platform manages the device and the redundancy. If the primary Routing Engine fails, the backup Routing Engine takes over and Junos Space Network Management Platform manages the transition automatically without bringing down the device.

NOTE: When you initiate discovery on a device running Junos OS, Junos Space Network Management Platform automatically enables the NETCONF protocol over SSH by pushing the following command to the device:

```
set system services netconf ssh
```

To create a device discovery profile, complete the following tasks:

1. Specifying Device Targets | 227
2. Specifying Probes | 230
3. Selecting the Authentication Method and Specifying Credentials | 233
4. (Optional) Specifying SSH Fingerprints | 235
5. Scheduling Device Discovery | 235

Specifying Device Targets

Device targets are IP addresses or hostnames of devices that you want Junos Space Network Management Platform to discover.

To specify the device targets that you want Junos Space Network Management Platform to discover:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Discovery > Device Discovery Profiles**.

   The Discover Discovery Profiles page is displayed.

2. Click the **Create Device Discovery Profile** icon on the toolbar.

   The Device Discovery Target page is displayed on the left. The list of different tasks that should be completed to create a profile is displayed on the right: Device Discovery Target, Specify Probes, Specify Credentials, Specify Device FingerPrint, and Schedule/Recurrence.

   NOTE: At any point in time, you can click the links to the different tasks (on the right of the page) and navigate to those pages.

3. In the Discovery Profile Name field, enter the name of the device discovery profile.

   The device discovery profile name cannot exceed 255 characters and can contain letters, numbers, spaces, and special characters. The special characters allowed are period (.), hyphen (-), and underscore

(_). The device discovery profile name cannot start with letters or numbers and cannot contain leading or trailing spaces.

> **NOTE:** The Make Public check box is selected by default so that the device discovery profile is visible to all users.

4. In the Discovery Parameters field, you can add devices manually by specifying the details on the Device Discovery Target page or by uploading the details of the devices through a CSV file.

   To add devices manually:

   a. Click the **Add Manually** option button.

b. In the Target Type area, select how you want to specify the targets: IP addresses or hostnames, IP ranges, or a subnet.

- To enter the IP address or hostname of the device:

  i. Select the **IP Address/Hostname** option button.

  ii. In the Target Details field, enter the IP address or hostname.

  > **NOTE:** You can enter the IP address in either IPv4 or IPv6 format. Refer to http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml for the list of restricted IPv6 addresses.

  > **NOTE:** You can enter a combination of the following separated by a comma (,):
  >
  > - IP addresses
  > - Hostnames
  > - IP address range expressions
  > - Subnet expressions
  >
  > For example, **192.168.27.1, example.abc.com, 192.168.27.50-192.168.27.60,192.168.26.0/24**

- To enter a range of IP addresses for the devices:

  i. Select the **IP Range** option button.

  The maximum number of IP addresses for an IP range target is 1024.

  ii. In the Start IP Address field, enter the first IP address.

  iii. In the End IP Address field, enter the last IP address.

- To enter an IP subnet for the devices:

  i. Select the **Subnet** option button.

  ii. In the IP Subnet/CIDR field, enter the subnet details.

The subnet prefix for IPv4 addresses is 1–32 and for IPv6 addresses is 1–128.

To add devices by using a CSV file:

> **NOTE:** Device discovery is supported only for existing public tags in Junos Space Platform.
>
> Starting from Junos Space Network Management Platform Release 16.1R1, a Private Key column has been added in the CSV file to support the custom key option for device discovery. Ensure that you use the latest sample CSV file. However, backward compatibility is supported. That is, if you use an existing CSV file (from a previous release), the file is uploaded successfully.

a. Click the **Upload CSV** option button.

> **NOTE:** The format of the CSV file that you are uploading should exactly match the format of the sample CSV file.
>
> You can add hundreds of devices to Junos Space Network Management Platform by using a CSV file. You can specify the hostnames, IP addresses, device login credentials, tags, and SSH fingerprints in the CSV file.

b. (Optional) To view a sample CSV file, click the **Sample CSV** link.

c. Click **Browse**.

   The CSV File Upload dialog box appears.

d. Navigate to the desired CSV file, select it, and then click **Open**.

   The name of the CSV file is displayed in the CSV File: field.

e. Click **Upload** to upload the selected CSV file.

5. Click **Next** to proceed and select probes.

   The **Specify Probes** page is displayed.

Specifying Probes

Probes are protocols used to find devices on the network—ping, SNMP, or SSH.

To specify probes on the Specify Probes page:

1. To use the NAT configuration to discover devices using this profile, select the the **Use NAT** check box.

   The Use NAT check box is available for selection only if NAT is already configured in Junos Space.

2. To discover devices using ping (if SNMP is not configured on the device), select the **Use Ping** check box.

   By default, this check box is selected.

3. To discover devices using SNMP (if SNMP is configured on the device), select the **Use SNMP** check box.

   By default, this check box is selected.

   NOTE: If you clear both the Use Ping and Use SNMP check boxes, SSH is used to discover devices. When both the Use Ping and Use SNMP check boxes are selected (the default), Junos Space Network Management Platform can discover the target device more quickly, but only if the device is pingable and SNMP is enabled on the device.

4. You can select an appropriate version of SNMP during discovery:
   - To use SNMP v1 or v2c:
     i. Select the **SNMP V1/V2C** option button.
     ii. Specify a community string, which can be **public**, **private**, or a predefined string.
     The default community string is **public**.
   - To use SNMP v3:
     i. Select the **SNMP V3** option button.
     ii. In the User Name field, enter the username.
     iii. In the Authentication type field, select the authentication type (**MD5**, **SHA1**, or **None**).
     iv. In the Authentication password field, enter the authentication password. .
     This field is available only if you selected MD5 or SHA1 in the Authentication type field. If you selected **None** as the authentication type, the authentication function is disabled.
     v. Select the privacy type (**AES128**, **AES192**, **AES256**, **DES**, or **None**).
     vi. Enter the privacy password (if AES128, AES192, AES256, or DES).
     If you specify **None** for the privacy type, the privacy function is disabled.

     NOTE: The SNMPv3 privacy mode supports Advanced Encryption Standard (AES) algorithms with 192-bit and 256-bit encryption from Junos Space Network Management Platform Release 16.1R1 onward.

5. (Optional) Click **Back** to navigate to the Device Discovery Target page and change the details of the device targets.

6. Click **Next** to proceed and select the authentication method.
   The **Specify Credentials** page is displayed.

Selecting the Authentication Method and Specifying Credentials

You can choose the mode of authentication for the devices you are about to discover. For credentials-based authentication, if you already specified the device login credentials in the CSV file, you can skip the Specify Credentials page. With credentials-based authentication, you can specify a common administrator name and password to establish an SSH connection to each target device that you are about to discover. If you are using key-based authentication, you must have generated keys from Junos Space Network Management Platform or must have the private key on your computer.

To specify the mode of authentication and credentials on the Specify Credentials page:

1. Select the mode of authentication used to authenticate devices during discovery.

   To use credentials-based authentication:

   a. In the Authentication Type area, select the **Credentials-Based Authentication** option button.

   b. In the Username field, enter the administrator username.

   c. In the Password field, enter the administrator password.

   d. In the Confirm Password field, reenter the administrator password.

   To use key-based authentication:

   a. In the Authentication Type area, select the **Key-Based Authentication** option button.

   b. In the Username field, enter the administrator username.

You can use a key generated from Junos Space Network Management Platform (known as Space Key) or a custom private key uploaded to Junos Space Network Management Platform:

- To use a key generated from Junos Space Network Management Platform:

  i. Select the **Use Space Key** option button.

  From Junos Space Platform Release 18.2 onward, you can upload Space Key for authentication to Junos Space Platform by using the device discovery workflow.

  Select the **Upload Space Key to Device** checkbox to upload the Space Key to the device.

  To upload Space Key:

  - Enter the username in the Authorized Username field.
  - Enter the password in the Authorized Password field.

  > **NOTE:** The above credentials, Authorized Username and Authorized Password, are used only to upload the Space Key to the device.
  >
  > If the username you specify in the Username field does not exist on the device, a user with this username is created as a super user and the key is uploaded for this user.

- To use a custom private key:

  i. Select the **Use Custom Key** option button.

  ii. (Optional) In the Passphrase field, enter the passphrase created when you generated the private key.

  iii. Next to the Private Key field, click the **Browse** button to upload the private key for the managed devices.

  > **NOTE:** If you modify the discovery profile, the Private Key field displays **id_rsa** (which is the default filename) instead of the name of the uploaded file.

c. (Optional) Click **Back** to navigate to the preceding pages and change the probes and device targets.

d. Click **Next** to proceed and specify device fingerprints.

The **Specify Device FingerPrint** page is displayed.

(Optional) Specifying SSH Fingerprints

Optionally, specify or modify (if you specified the fingerprints by using the CSV file) the SSH fingerprints for target devices. If you do not specify the fingerprints, Junos Space Network Management Platform obtains fingerprint details when it connects to the device for the first time. You can specify fingerprints during device discovery only for Juniper Networks devices. If you already specified the SSH fingerprints in the CSV file, you can skip this task.

To specify the SSH fingerprints on the Specify Device FingerPrint page:

1. Click the Fingerprint column corresponding to the device and enter the SSH fingerprint of the device.

   NOTE: You can specify fingerprints for a maximum of 1024 devices simultaneously using this workflow.

2. (Optional) Repeat step 1 for all devices or devices whose fingerprints you know.

3. (Optional) Click **Back** to navigate to the preceding pages and change the authentication details, probes, and device targets.

4. Click **Next** to proceed and schedule discovery by using this profile.

   The **Schedule/Recurrence** page is displayed.

Scheduling Device Discovery

Schedule the device discovery profile to discover devices to Junos Space Network Management Platform.

To schedule the device discovery profile to discover devices:

1. Select the **Schedule at a later time** check box.
   a. Enter the date in the Date field in the MM/DD/YYYY format.

b. Enter the time in the Time field in the hh:mm format.

2. Select the **Recurrence** check box.
   a. (Optional) Select the periodicity of recurrence from the Repeats list.

      The options are Minutes, Hourly, Daily, Weekly, Monthly, and Yearly. The default is Weekly.

   b. (Optional) Select the interval from the Repeat every list.

      The default is 1.

   c. (Optional) If you select Weekly from the Repeats list, the Repeat by field appears. Select the check boxes for the days of the week that you want the job to recur.

   d. (Optional) Click the On option button in the Ends field to specify an end date for the job recurrence.

      If you select the Never option button, the job recurs endlessly until you cancel the job manually.

   e. To specify the date and time when you want to end the job recurrence:
      i. Enter the date in the Date field in the MM/DD/YYYY format.

      ii. Enter the time in the Time field in the hh:mm format.

3. (Optional) Click **Back** to navigate to the preceding page and change fingerprints, authentication details, probes, and device targets.

4. Click **Finish** to save the device discovery profile.

   A job is created and the Discover Network Elements Information dialog box displays the link to the job ID. Click **OK** to close the Information dialog box.

Release History Table

Release	Description
18.2	From Junos Space Platform Release 18.2 onward, you can upload Space Key for authentication to Junos Space Platform by using the device discovery workflow.
16.1R1	Starting from Junos Space Network Management Platform Release 16.1R1, a Private Key column has been added in the CSV file to support the custom key option for device discovery.
16.1R1	The SNMPv3 privacy mode supports Advanced Encryption Standard (AES) algorithms with 192-bit and 256-bit encryption from Junos Space Network Management Platform Release 16.1R1 onward.

RELATED DOCUMENTATION

- Understanding How Junos Space Automatically Resynchronizes Managed Devices | **216**
- Device Discovery Profiles Overview | **220**
- Exporting the Device Discovery Details As a CSV File | **245**
- Viewing Managed Devices | **194**
- Viewing Jobs | **972**
- Resynchronizing Managed Devices with the Network | **448**
- Viewing the Physical Inventory | **301**
- Viewing Physical Interfaces of Devices | **306**
- Exporting the License Inventory | **312**
- DMI Schema Management Overview | **1534**
- Device Authentication in Junos Space Overview | **281**

Running Device Discovery Profiles

You run a device discovery profile to automatically discover, synchronize device inventory and interface details, and manage devices running Junos OS to Junos Space Network Management Platform. Device discovery is a four-step process in which you specify target devices, credentials to connect to each device (that is, reuse existing credentials or specify new ones), and, optionally, the probe method (ICMP Ping, SNMP, both ICMP Ping and SNMP, or none), and the SSH fingerprint for each device. You can run multiple device discovery profiles by using this workflow. If you run multiple device discovery profiles, all devices targets specified in the device discovery profiles are discovered.

Before you start discovering devices, ensure that the following conditions are met:

- The device is configured with a management IP address that is reachable from the Junos Space server, or the NAT server if you are using a NAT server on your Junos Space setup.
- A user with the privileges of a Junos Space administrator is created and enabled on the device.
- The device is configured to respond to ping requests if you intend to use ping as the probe method to discover devices.
- SNMP is enabled on the device with appropriate read-only v1 or v2c or v3 credentials if you intend to use SNMP as the probe method to discover devices.

> **NOTE:** To discover and manage a cluster of SRX Series devices, each cluster node must be discovered independently using the management IP address of the respective node.

To run discovery profiles:

1. On the Junos Space Network Management Platform user interface, select **Devices >Device Discovery > Device Discovery Profiles**.

   The Discover Discovery Profiles page is displayed.

2. Select the check boxes corresponding to the discovery profiles you want to run and click the **Run Now** icon on the toolbar.

   The Discovery Status report appears. This report shows the progress of discovery in real time. Click a bar in the chart to view information about the devices currently managed or discovered, or for which discovery failed.

   A job is created for every device discovery profile you run. From the Job Details page, you can check whether a device was discovered and added to Junos Space Network Management Platform. If a device is discovered, you can view the device on the Device Management page.

   To go to the Job Details page, double-click the ID of the device discovery job on the Job Management page. The Description column on this page specifies whether the device was discovered and added to

Junos Space Network Management Platform. If the device was not discovered and added to Junos Space Network Management Platform, the column lists the reason for failure. You can also sort all the columns in ascending or descending order to identify the devices that are discovered and devices that are not discovered.

To export the device discovery details for all device discovery profiles that are run, from the Job Details page, see "Exporting the Device Discovery Details As a CSV File" on page 245.

Verify the following changes in the Web UI to ensure that the clusters are discovered successfully:

- In the **Manage Devices Inventory** page:

  Each peer device displays the other cluster member.

  The devices are displayed as primary and secondary in the cluster.

- In the **Physical Inventory** page:

  The chassis information is displayed for each peer device in the cluster.

RELATED DOCUMENTATION

Creating a Device Discovery Profile | 226

Device Discovery Profiles Overview | 220

Viewing a Device Discovery Profile | 243

Exporting the Device Discovery Details As a CSV File | 245

Modifying a Device Discovery Profile

You modify a device discovery profile when you want to expand the range of device targets, change device targets when devices were not discovered, change credentials or other details such as fingerprints or the discovery schedule.

NOTE: Ensure that you have no discovery jobs scheduled for a device discovery profile that you want to modify. All discovery jobs scheduled from the original device discovery profile are canceled after you modify the original device discovery profile.

To modify a device discovery profile:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Discovery > Device Discovery Profiles**.

   The Discover Discovery Profiles page is displayed.

2. Select the check box corresponding to the device discovery profile you want to modify and click the **Modify Profile** icon on the toolbar

   The Modify Device Discovery Profile page is displayed.

   The Device Discovery Target page is displayed on the left. The list of different tasks that should be completed to create a device discovery profile is displayed on the right: Device Discovery Target, Specify Probes, Specify Credentials, Specify Device FingerPrint, and Schedule/Recurrence.

   > **NOTE:** At any point in time, you can click the links to the different tasks (on the right of the page), navigate to those pages, and modify the details of the device discovery profile.

3. (Optional) Review and modify the details of the device and click **Next**.

   The **Specify Probes** page is displayed.

4. (Optional) Review and modify the probes and click **Next**.

   The **Specify Credentials** page is displayed.

5. (Optional) Review and modify the authentication details and click **Next**.

   > **NOTE:** If you modify the discovery profile, the Private Key field displays **id_rsa** (which is the default filename) instead of the name of the uploaded file.

   The **Specify Device FingerPrint** page is displayed.

6. (Optional) Review and modify the fingerprint details and click **Next**.

   The **Schedule/Recurrence** page is displayed.

7. Review and modify the schedule and click **Finish**.

   The device discovery profile is modified. A job is created and the Discover Network Elements Information dialog box displays the link to the job ID. Click **OK** to close the Information dialog box.

NOTE: If you modify and run a device discovery profile for which an associated device discovery job is already in progress, the existing job is cancelled and a new job is triggered for the modified discovery profile.

RELATED DOCUMENTATION

- Creating a Device Discovery Profile | 226
- Running Device Discovery Profiles | 238
- Viewing a Device Discovery Profile | 243
- Deleting Device Discovery Profiles | 244

Cloning a Device Discovery Profile

You clone a device discovery profile when you want to reuse the details of an existing device discovery profile and quickly create a new device discovery profile.

NOTE: To use the cloned device discovery profile immediately after cloning, you must not modify the targets and fingerprints, or the discovery schedule. You can also choose not to schedule discovery until you finalize the discovery preferences.

To clone a device discovery profile:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Discovery > Device Discovery Profiles**.

   The Discover Discovery Profiles page is displayed.

2. Select the check box corresponding to the device discovery profile you want to clone and click **Clone Profile** from the Actions menu.

   The Clone Device Discovery Profile page is displayed.

   The Device Discovery Target page is displayed on the left. The list of different tasks that should be completed to create a device discovery profile is displayed on the right: Device Discovery Target, Specify Probes, Specify Credentials, Specify Device FingerPrint, and Schedule/Recurrence.

> **NOTE:** At any point in time, you can click the links to the different tasks (on the right of the page), navigate to those pages, and change the details of the device discovery profile.

3. (Optional) Review and modify the details of the device and click **Next**.

   The **Specify Probes** page is displayed.

4. (Optional) Review and modify the probes and click **Next**.

   The **Specify Credentials** page is displayed.

5. (Optional) Review and modify the authentication details and click **Next**.

   > **NOTE:** If you modify the discovery profile, the Private Key field displays **id_rsa** (which is the default filename) instead of the name of the uploaded file.

   The **Specify Device FingerPrint** page is displayed.

6. (Optional) Review and modify the fingerprint details and click **Next**.

   The **Schedule/Recurrence** page is displayed.

7. (Optional) Review and modify the schedule and click **Finish**.

   A new device discovery profile is created. A job is created and the Discover Network Elements Information dialog box displays the link to the job ID. Click **OK** to close the Information dialog box.

RELATED DOCUMENTATION

- Creating a Device Discovery Profile | 226
- Running Device Discovery Profiles | 238
- Modifying a Device Discovery Profile | 239
- Viewing a Device Discovery Profile | 243

Viewing a Device Discovery Profile

You view a device discovery profile when you want to see the details of the device discovery profile.

To view the details of a device discovery profile:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Discovery Profiles**.

   The Discover Discovery Profiles page is displayed.

2. Select the check box corresponding to the device discovery profile you want to view and click the **View Profile** on the toolbar.

   The View Discovery Profile pop-up window is displayed.

   Table 21 displays the fields in the View Discovery Profile pop-up window.

   Table 21: View Discovery Profile Pop-up Window

Field	Description
Profile Name	Name of the device discovery profile
Visibility	Whether public or private
Target Type	Whether the discovery target for devices is specified as an IP address, hostname, IP range, or subnet
Target Details	Combination of IP addresses and hostnames, IP range, and IP subnet details of the devices
Credential Type	Type of credentials: key based, credential based, or custom key based
Username	Administrator username used to discover the device
Use Ping	Whether ping is enabled for device discovery
Use SNMP	Whether SNMP is enabled for device discovery
SNMP Version	Version of SNMP used: v1 or v2c, or v3

3. Click **Close** to close the pop-up window.

RELATED DOCUMENTATION

Modifying a Device Discovery Profile | 239

Cloning a Device Discovery Profile | 241

Creating a Device Discovery Profile | 226

Running Device Discovery Profiles | 238

Deleting Device Discovery Profiles

You delete device discovery profiles when you no longer want to save them in the Junos Space Network Management Platform database.

NOTE: If you delete a device discovery profile, all discovery jobs scheduled for the device discovery profile are canceled.

To delete device discovery profiles:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Discovery > Device Discovery Profiles**.

   The Discover Discovery Profiles page is displayed.

2. Select the check boxes corresponding to the device discovery profiles you want to delete and click the **Delete Profile** icon on the toolbar

   The Delete Device Discovery Profile pop-up window is displayed.

3. You can either delete or retain the device discovery profiles.

   - Click **Delete** in the Delete Device Discovery Profile pop-up window.

     The device discovery profiles are deleted.

   - Click **Cancel** to retain the device discovery profiles on Junos Space Platform.

RELATED DOCUMENTATION

Viewing a Device Discovery Profile | 243

Creating a Device Discovery Profile | 226
Running Device Discovery Profiles | 238

Exporting the Device Discovery Details As a CSV File

A job is triggered when you discover one or multiple devices by using a device discovery profile—either manually using the Run Now option or through discovery scheduled when creating the device discovery profile. You can export the results of the device discovery job from the Job Management page as a CSV file. You can view the hostname, IP address, status, and description of the devices listed in the device discovery job in the CSV file.

To export the device discovery job details as a CSV file:

1. On the Network Management Platform user interface, select **Jobs > Job Management**.
2. Double-click the device discovery job whose details you want to export as a CSV file.
3. Click **Export as CSV**.

   You are prompted to save the file.
4. Click **OK** on the File Save dialog box to save the file to your local file system.
5. After you save the file, to return to the Job Management page, click the [X] icon on the Exporting Discovery Job.

RELATED DOCUMENTATION

Running Device Discovery Profiles | 238
Device Discovery Profiles Overview | 220
Creating a Device Discovery Profile | 226
Modifying a Device Discovery Profile | 239
Viewing a Device Discovery Profile | 243

CHAPTER 10

Modeling Devices

IN THIS CHAPTER

- Rapid Deployment Overview | **247**
- Zero Touch Deployment Using Autoinstallation and Junos Space Network Management Platform on ACX Series and SRX Series Devices | **248**
- Model Devices Overview | **251**
- Creating a Connection Profile | **252**
- Creating a Modeled Instance | **257**
- Activating a Modeled or Cloned Device in Junos Space Network Management Platform | **262**
- Downloading a Configlet | **266**
- Viewing and Copying Configlet Data | **268**
- Activating Devices by Using Configlets | **269**
- Viewing a Modeled Instance | **272**
- Adding More Devices to an Existing Modeled Instance | **274**
- Viewing the Status of Modeled Devices | **275**
- Deleting Modeled Instances | **276**
- Viewing a Connection Profile | **276**
- Cloning a Connection Profile | **278**
- Modifying a Connection Profile | **278**
- Deleting Connection Profiles | **279**

Rapid Deployment Overview

The Junos Space Rapid Deployment solution enables you to model Juniper Networks devices quickly and effectively from Junos Space Network Management Platform. Devices are modeled by using the Model Devices workflow in the Devices workspace. When you add physical devices to your network, you can activate the modeled devices and associate the physical devices to the modeled devices. If you are deploying a ACX Series or SRX Series device, you can use the autoinstallation feature during deployment. For more information, see "Zero Touch Deployment Using Autoinstallation and Junos Space Network Management Platform on ACX Series and SRX Series Devices" on page 248.

Devices are either activated from Junos Space Platform (by using the Activate workflow) or by using the configlets (also known as one-touch deployment) generated from the Create Modeled Instance workflow. By default, configlets contain the minimum initial configuration (connection parameters) for modeled devices to connect to Junos Space Platform. The minimum initial configuration includes the FQDN of Junos Space, SSH secure key to access the device from Junos Space Platform, ID of the device, keep-alive timer, WAN IP configuration: static or DHCP, and default gateway and DNS details.

If you associate the modeled instance with a device template and select to update a device template manually, the configlet contains the configuration in the device template in addition to the minimum initial configuration.

Following are the six steps that outline the Rapid Deployment solution in Junos Space Platform:

1. Create a modeled instance that defines the number of devices that will be added to the Junos Space Platform database. You can assign a hostname, IP address, subnet mask, platform, and serial number on a per-device basis. Refer to "Creating a Modeled Instance" on page 257 for more information.
2. Generate a configlet and Initiate a connection between Junos Space Platform in one of the following ways:
   - Copy the contents of the configlet generated by the modeled instance to the CLI console of the device. When this initial configuration is committed on the device, the device connects to Junos Space Platform.
   - Connect the USB device containing the configlet to the device and reboot the device. The device then connects to Junos Space Platform. Refer to "Activating Devices by Using Configlets" on page 269 for more information.
   - Initiate the workflow to activate the modeled instance that contains the device. Refer to "Activating a Modeled or Cloned Device in Junos Space Network Management Platform" on page 262 for more information.
3. When the device boots up and connects to the WAN link, an IP address is assigned to the device depending on the connection profile you assigned to the modeled instance containing the device.
4. The device connects to Junos Space Platform through an SSH session.

5. Junos Space Platform authenticates the device and optionally validates the serial number and hostname of the device. The device is managed in Junos Space Platform only if the validation succeeds. If the validation fails, the device is not managed in Junos Space Platform.
6. Junos Space Platform either upgrades or downgrades the Junos OS version of the device if you select the **Image Upgrade/Downgrade** check box in the Model Devices workflow.

   Junos Space Platform also pushes additional configuration settings through device templates if you select the **Template Association** check box and choose to update the configuration automatically. If you select a manual update of the device configuration, you must load the configlets to the device through a USB device or an FTP server.

RELATED DOCUMENTATION

Model Devices Overview | 251

Creating a Modeled Instance | 257

Activating a Modeled or Cloned Device in Junos Space Network Management Platform | 262

Viewing and Copying Configlet Data | 268

Zero Touch Deployment Using Autoinstallation and Junos Space Network Management Platform on ACX Series and SRX Series Devices

IN THIS SECTION

- Zero-Touch Deployment Using the Autoinstallation and Model and Activate Devices Features | 250
- Zero-Touch Deployment Using the Autoinstallation Feature and the Configuration Server | 250

Zero-touch deployment means that you can deploy new Juniper Networks ACX Series and SRX Series devices in your network automatically, without manual intervention. When you physically connect a device to the network and boot it with a default factory configuration, the device attempts to upgrade the Junos OS software automatically and autoinstall a configuration file from the network. Zero-touch deployment of devices that are discovered to Junos Space Platform can be performed by using the built-in autoinstallation feature in case of ACX Series routers or SRX Series devices or by using the Model and Activate devices feature in Junos Space Platform.

Zero-touch deployment provides the following benefits:

- The device can be sent from the warehouse to the deployment site without any preconfiguration steps.
- The procedure required to deploy the device is simplified, resulting in reduced operational and administrative costs.
- You can roll out large numbers of these devices in a very short time.

Autoinstallation provides automatic configuration for a new device that you connect to the network and turn on, or for any existing device configured for autoinstallation. This autoinstallation mechanism allows the new device to configure itself out-of-the-box with no manual intervention, using the configuration available on the network, locally through USB storage media, or a combination of both. Autoinstallation takes place automatically when you connect a device to the network and power on the device. The autoinstallation feature enables you to deploy multiple devices from a central location in the network.

The autoinstallation process begins when a device is powered on and cannot locate a valid configuration file in the CompactFlash card. Typically, a configuration file is unavailable when a device is powered on for the first time, or if the configuration file is deleted from the CompactFlash card. For the autoinstallation process to work, you must store one or more host-specific or default configuration files on a configuration server in the network and have a service available—typically, Dynamic Host Configuration Protocol (DHCP)—to assign an IP address to the device. To simplify the process, you can explicitly enable autoinstallation on a device and specify a configuration server, an autoinstallation interface, and a protocol for IP address acquisition.

The autoinstallation process operates in three modes:

- Network Mode—Autoinstallation triggers IP address acquisition mechanism (the device sends out Dynamic Host Configuration Protocol [DHCP] or Reverse Address Resolution Protocol [RARP] requests on each connected interface simultaneously) to obtain an IP address. After the device has an IP address, the device sends a request to the specified configuration server and downloads and installs the configuration.
- USB mode—Autoinstallation obtains the required configuration from the configuration file saved in an external USB storage device plugged into the device. The USB-based autoinstallation process overrides the network-based autoinstallation process. If the device detects a USB storage device containing a valid configuration file during autoinstallation, the device uses the configuration file on the USB storage device instead of fetching the configuration from the network. For more information, refer to USB Autoinstallation on ACX Series Routers.
- Hybrid mode—Autoinstallation obtains partial configuration from an external USB storage device and uses that configuration to obtain the complete configuration file in network mode. This mode is a combination of USB mode and Network mode.

For more information about the prerequisites for the autoinstallation and the autoinstallation process, refer to the following topics:

- ACX Series router autoinstallation overview—ACX Series Autoinstallation Overview
- SRX Series device autoinstallation overview—SRX Series Autoinstallation Overview

- Prerequisites for autoinstallation on an ACX Series router—Before You Begin Autoinstallation on an ACX Series Router
- Autoinstallation on an SRX Series device—Configuring Autoinstallation on SRX Series Devices

> **NOTE:** To make sure that you have the default factory configuration loaded on the device, issue the **request system zeroize** command on the device that you want to deploy.

This topic contains the following sections:

Zero-Touch Deployment Using the Autoinstallation and Model and Activate Devices Features

For zero-touch deployment using the autoinstallation and the Model and Activate devices features, you can create connection profiles and configlets from the Junos Space Platform UI. The configlets should be deployed on the devices in the network topology by using a USB storage device. You can modify the configuration of a modeled device by using the Device Templates feature from the Junos Space Platform UI, before deploying the configlets to the device. You can use the Model and Activate devices feature to install Junos OS software on different devices with minimal manual supervision.

The Model and Activate Devices feature comprises the following operations:

1. (Optional) Creating connection profiles (see “Creating a Connection Profile” on page 252)
2. Creating modeled instances (see “Creating a Modeled Instance” on page 257)
3. Performing configuration changes on a device (see “Modifying the Configuration on the Device” on page 322)
4. Activating the model device (see “Activating a Modeled or Cloned Device in Junos Space Network Management Platform” on page 262)

Zero-Touch Deployment Using the Autoinstallation Feature and the Configuration Server

You can use a configuration server with scripts, configuration files, and the DHCP feature enabled, and the autoinstallation feature for zero-touch deployment. In this case, you need not use Junos Space Platform to update the configuration and Junos OS software on the device. The device uses information that you configure on a configuration server (DHCP server) to locate the necessary Junos OS software image and configuration files on the network. If you do not configure the configuration server to provide this information, the device boots with the preinstalled software and the default factory configuration.

Zero-touch deployment using autoinstallation comprises the following operations:

1. (Optional) Creating connection profiles (see "Creating a Connection Profile" on page 252)
2. Creating modeled instances (see "Creating a Modeled Instance" on page 257 and "Activating a Modeled or Cloned Device in Junos Space Network Management Platform" on page 262)
3. Downloading configlets (see "Viewing and Copying Configlet Data" on page 268 and "Downloading a Configlet" on page 266)
4. Deploying configlets on devices at the network site (see "Activating Devices by Using Configlets" on page 269)

RELATED DOCUMENTATION

Rapid Deployment Overview | 247

Model Devices Overview | 251

Downloading a Configlet | 266

Viewing and Copying Configlet Data | 268

Activating Devices by Using Configlets | 269

Model Devices Overview

With the Model Devices feature, you can add multiple devices, specify connectivity parameters, upgrade schema-based configuration on the devices, and upgrade or downgrade the Junos OS version on the devices through a single workflow. This workflow creates a modeled instance and adds the devices to Junos Space Network Management Platform. Devices added using this workflow are known as modeled devices. You then activate these devices by initiating a connection from Junos Space or the device, or by manually copying the configlets to the devices and allowing the devices to connect back to Junos Space Platform. When the activation is complete, the devices can be managed from Junos Space Platform. You can also activate the devices when creating the modeled instance, using the Activate Now option. This option is available only for activation using a device initiated connection and the device is assigned the Waiting for deployment state on the Device Management table. If you choose to activate the device later, the device is assigned the Modeled state on the Device Management page.

Using the Model Devices feature, you can create a connection profile to specify a set of connectivity parameters of a device. A connection profile specifies the details of the device interface on which the IP address is configured, the NAT configuration details for Junos Space Platform, and the details of the protocol used to assign IP addresses to the devices. You can create a modeled instance using this connection profile. Devices created using this modeled instance use the common connectivity parameters specified in the connection profile. You can model devices both in the IPv4 and IPv6 formats.

A modeled instance is a set of modeled devices that share the same connection profile. A modeled instance defines the device family for which the configlets are applicable, the Junos OS version that the device will be upgraded or downgraded to, if needed, and the device template containing the common configuration that you want to push to the devices when they are discovered in Junos Space Platform.

You can activate the modeled devices immediately after they are added to Junos Space Platform. Use a Junos Space–initiated connection or device–initiated connection to connect to and activate these devices. If you use a device–initiated connection, you need to specify the credentials to manage the device in Junos Space Platform after the device connects to Junos Space Platform. If you use a Junos Space–initiated connection to activate the device, you need to specify the hostname or IP address details and user credentials for Junos Space Platform to initiate the connection to the device. You can also specify a different set of user credentials to connect to the device than the one used to manage the device on Junos Space Platform. You can choose whether to update the configuration on the device automatically during the activation or manually.

RELATED DOCUMENTATION

Rapid Deployment Overview | 247

Creating a Connection Profile | 252

Creating a Modeled Instance | 257

Creating a Connection Profile

You use a connection profile to specify connectivity-related parameters for devices added to Junos Space Network Management Platform using the Modeling devices feature. A connection profile contains device interface details, and the protocol used to assign IP addresses to devices. If you choose to use a NAT server between managed devices and Junos Space Platform, the connection profile uses the NAT configuration configured in the Administration workspace. You create connection profiles from the Connection Profiles page in the Devices workspace.

To create a connection profile:

1. On the Network Management Platform user interface, select **Devices > Model Devices > Connection Profiles**.

   The Connection Profiles page is displayed.

2. Click the Create Connection Profile icon on the Actions menu.

   The Create Connection Profile page is displayed.

3. In the Name field, enter a name for the new connection profile.

   The connection profile name cannot exceed 255 characters and can contain letters, numbers, spaces, and special characters. The special characters allowed are period (.), hyphen (-), and underscore (_). The connection profile name cannot start with letters or numbers and cannot contain leading or trailing spaces.

4. (Optional) In the Description field, enter a description for the new connection profile.

   The description cannot exceed 256 characters.

5. Select the type of device interface on which you want to configure the IP address: **Ethernet**, **ADSL**, or T1.

   By default, the Ethernet option button is selected.

6. (Optional) In the Interface field, enter the appropriate device interface number.

   The default Ethernet interface number is ge-0/0/0. The default ADSL interface number is at-1/0/0.

7. Select the format of the IP address for the devices to be modeled using this connection profile. By default, the **IPv4** option button is selected.

   - If you want to model devices by using an IPv6 address, select the **IPv6** option button.

   NOTE: The contents of the configlet generated differ based on the format of the IP address.

8. (Optional) Select the **NAT'd IP Address for Junos Space** check box to use the NAT configuration specified in the Administration workspace.

   By default, this check box is cleared. If you are not using a NAT server or have disabled or not enabled the NAT configuration, this field is dimmed.

   NOTE: You need to configure the NAT server with the same format of the IP address that you chose to model devices by using this connection profile.

   Refer to http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml for the list of restricted IPv6 addresses.

9. (Optional) From the **IP Assignment via** drop-down list, select how the IP address is assigned to the devices. By default, DHCP is selected. The options presented hereafter depend on the type of device interface on which you configure the IP address and how the IP address is assigned to the devices.

   You can assign IP addresses by using the following options for Ethernet and T1 interface:

   - Manually (Static)
   - Dynamic Host Configuration Protocol (DHCP)
   - Point-to-Point Protocol over Ethernet (PPPoE)

   You can assign IP addresses by using the following options for the ADSL interface:

   - Manually (Static)
   - Dynamic Host Configuration Protocol (DHCP)
   - Point-to-Point Protocol over ATM (PPPoA)

   If you want to assign an IP address to the device manually:

   - Select **Static** from the **IP Assignment via** drop-down list

     If you select Static, you should enter the IP addresses of the devices manually when you create a modeled instance.

   If you select **DHCP** from the drop-down list:

   a. From the **Attempts** selector, use the up and down arrows to specify the maximum number of attempts that the DHCP server will make to reconfigure the DHCP clients before the reconfiguration is considered to have failed.

      The default value is 4 attempts.

   b. From the **Interval** selector, use the up and down arrows to specify the initial value in seconds between successive attempts to reconfigure the DHCP clients.

      The default value is 4 seconds.

   c. (Optional) Select the **DHCP Server Address** check box to configure the properties of the DHCP server.

   d. In the IP Address field, enter the IP address of the DHCP server.

      NOTE: You can enter the IP address in either IPv4 or IPv6 format.

   e. If you want the DHCP clients to propagate the TCP/IP settings to the DHCP server, select the **Update Server** check box.

   f. Select one of the option buttons in the Lease Time section: **Default Value**, **Lease Never Expires**, or **Lease time**. By default, the Default Value option button is selected.

This option specifies the time taken by the DHCP server to negotiate and exchange DHCP messages with the DHCP clients.

- If you want the DHCP server to negotiate and exchange DHCP messages with the DHCP clients, select the **Default Value** option button.
- If you want the DHCP server to assign permanent IP addresses, select the **Lease Never Expires** option button.
- If you want to specify a time interval after which the lease expires, select the Lease Time option button and use the up and down arrows in the **Interval** selector to specify the time interval.

  The default value is 4 seconds.

If you select **PPPoE** from the drop-down list:

a. From the **Authentication Type** drop-down list, select the type of authentication.

   Junos Space Network Management Platform supports Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) for authentication.

b. In the Username field, enter the username for PPPoE authentication using CHAP.

c. In the Password field, enter the password for PPPoE authentication using CHAP.

d. In the Confirm Password field, reenter the password for PPPoE authentication using CHAP.

e. In the Access Profile Username field, enter the username for PPPoE authentication.

   This field is not mandatory for PAP authentication.

f. In the Access Profile Password field, enter the password for PPPoE authentication.

   This field is not mandatory for PAP authentication.

g. In the Access Profile Confirm Password field, reenter the password for PPPoE authentication.

   This field is not mandatory for PAP authentication.

h. (Optional) In the Concentrator Name field, enter the name of the concentrator.

i. (Optional) In the Service Name field, enter the name of the service you are using.

j. In the **Auto Connect time Interval** field, use the up and down arrows to specify the time interval in seconds for connecting automatically. The default value is 1 second.

k. In the **Ideal time before disconnect** field, use the up and down arrows to specify the time interval in seconds before disconnecting. The default value is 1 second.

If you select **PPPoA** from the drop-down list:

a. From the **Authentication Type** drop-down list, select the type of authentication.

   Junos Space Network Management Platform supports Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) for authentication.

b. In the Username field, enter the username for PPPoE authentication using CHAP.

c. In the Password field, enter the password for PPPoE authentication using CHAP.

d. In the Confirm Password field, reenter the password for PPPoE authentication using CHAP.

e. In the Access Profile Username field, enter the username for PPPoE authentication.

   This field is not mandatory for PAP authentication.

f. In the Access Profile Password field, enter the password for PPPoE authentication.

   This field is not mandatory for PAP authentication.

g. In the Access Profile Confirm Password field, reenter the password for PPPoE authentication.

   This field is not mandatory for PAP authentication.

h. In the **VPI** field, use the up and down arrows to specify the Virtual Private Identifier (VPI) for the DSL network of your service provider. The range is 1 to 6000. The default value is 1.

i. In the **VCI** field, use the up and down arrows to specify the Virtual Channel Identifier (VCI) for the DSL network of your service provider. The range is 1 to 6000. The default value is 1.

j. From the **Encapsulation Type** drop-down list, select the type of encapsulation: atm-ppp-vc-mux or atm-ppp-llc. atm-ppp-vc-mux provides PPP over ATM AAL5 multiplex encapsulation and atm-ppp-llc provides PPP over AAL5 LLC encapsulation.

10. Click **Create**.

    The connection profile is created.

RELATED DOCUMENTATION

Modifying a Connection Profile | **278**

Deleting Connection Profiles | **279**

Creating a Modeled Instance | **257**

Creating a Modeled Instance

You create a modeled instance when you want to quickly add multiple devices to Junos Space Network Management Platform using a common set of connectivity parameters. You add a modeled instance from the Devices workspace.

To create a modeled instance:

1. On the Junos Space Network Management Platform user interface, select **Devices > Model Devices**.

   The Model Devices page is displayed.

2. Click the Create Modeled Instance icon on the toolbar.

   The Create Modeled Instance page is displayed.

3. From the **Device Type** drop-down list, select the type of device.

4. In the **Name** field, enter a name for the modeled instance.

   The modeled instance name should start and end with letters or numbers and cannot exceed 255 characters. The hyphen (-) and underscore (_) are the only special characters allowed. Leading and trailing spaces are not allowed.

5. In the **Description** field, enter a description of the modeled instance.

6. In the **Tag** field, enter a tag for the modeled instance and the modeled devices created in this modeled instance.

7. For Discovery Type, select **Add Manually** or **Upload CSV** to provide the details of the devices to be modeled.

   - If you want to provide the details of the devices manually, select the **Add Manually** option button.

     a. In the **Number of Devices** field, use the up and down arrows to specify the number of devices to be modeled using the modeled instance.

        The default value is 1.

     b. From the **Platform** drop-down list, select the platform for the devices.

   - If you want to provide the details of the devices through a CSV file, select the **Upload CSV** option button.

a. (Optional) Click the **View Sample CSV** link to download a sample CSV file.

   You need to retain the format of the CSV file for the devices to be modeled successfully. You need to enter the name of the devices and the platform of the devices in the CSV file.

   > **NOTE:** You need to retain the file format as .csv to successfully upload the details of the devices to Junos Space Network Management Platform.

b. Click the **Select a CSV To Upload** link to upload a CSV file.

   The Select CSV File pop-up window is displayed.

c. Click the **Browse** button to look for the file on your computer.

d. Click **Upload** to upload the CSV file to Junos Space Network Management Platform.

8. Select the the SNMP Settings check box and then, select either **V1/V2C** or **V3** to specify the version of SNMP to gather information from devices.

   By default, V1/V2C is selected.

   If you select **V1/V2C**:

   - Enter the SNMP community string in the **Community** field.

     By default, the public string is selected.

   If you select **V3**:

   a. In the **User Name** field, enter the username.

      The username can contain a maximum of 32 alphanumeric characters including spaces and symbols.

   b. From the **Authentication type** drop-down list, select the algorithm used for authentication. The options available are **MD5**, **SHA1**, or **None**.

   c. If you selected **MD5** or **SHA1**, enter the password in the **Authentication password** field.

      If you select **None**, this field is disabled.

      The following fields are displayed only if you choose an authentication algorithm.

      i. (Optional) From the **Privacy Type** drop-down list, select the algorithm used for encryption. The options available are **AES 128**, **AES 192**, **AES 256**, **DES**, or **None**.

      ii. (Optional) If you selected **AES 128**, **AES 192**, **AES 256**, or **DES**, enter the password in the **Privacy password** field.

If you select **None**, this field is disabled.

9. (Optional) Push the initial configuration to the devices after the devices are discovered on Junos Space Network Management Platform.
   a. Select the **Template Association** check box.
   b. From the **Device Template** drop-down list, select the appropriate device template that contains the configuration that you want to send to the devices.

   NOTE: The **Device Template** drop-down list does not list Quick templates with variables.

10. (Optional) Upgrade or downgrade to a common Junos OS version on all devices added using the modeled instance.
    a. Select the **Image Upgrade/Downgrade** check box.
    b. From the **Device Image** drop-down list, select the device image that contains the Junos OS version to which you want to upgrade or downgrade the devices.
11. Activate the devices immediately or later.

    NOTE: Junos Space Platform assigns the Waiting for Deployment state when devices are modeled using the Activate Now option and assigns the Modeled state when devices are modeled without the Activate Now option. You can activate devices using the Activate Now option only by using the device–initiated connection process.

    - To activate the devices immediately, select the **Activate Now** check box. This check box is selected by default.

      Enter the following data related to the activation of these devices:

      i. In the **Username** field, enter the username used to manage to the device.

         The username can contain two through 64 alphanumeric characters. The special characters allowed are hyphen (-) and underscore (_). The username must start with a nonhyphen character.

      ii. (Optional) Select the **Key Based Authentication** check box to use RSA keys for authentication.

         By default, this check box is not selected.

      iii. In the **Password** field, enter the password used to manage the device.

         The maximum length is 20 characters, the minimum length is six characters, and all characters are allowed.

iv. In the **Confirm Password** field, reenter the password.

v. (Optional) Select the **Serial Number Validation** check box to authenticate the device by using the serial number of the device.

   By default, this check box is not selected.

vi. (Optional) Select the **Host Name Validation** check box to authenticate the device by using the hostname.

   By default, this check box is not selected.

vii. (Optional) From the **Connection Profile** drop-down list, select a connection profile that specifies the connectivity parameters that you want to use for this modeled instance.

viii. (Optional) If you have not created a connection profile or want to create a new connection profile for this modeled instance, click the **Create** button next to the Connection Profile drop-down list.

   The Connection Profile pop-up window is displayed. For more information about creating a connection profile, see "Creating a Connection Profile" on page 252.

ix. Select whether you want to automatically push the device template configuration to the device from Junos Space Platform immediately or manually later. The **Configuration Update** options are **Automatic** and **Manual**.

   These options are disabled by default. They are active only if you have chosen the **Template Association** option earlier.

   - If you choose **Automatic**, the configuration is deployed to the device when the device is discovered to Junos Space Network Management Platform.

     This option is enabled by default.

   - If you choose **Manual**, you must load the complete configlet (i.e., you must download the configlet from Device Management ILP), which includes the device template configuration, through a USB device, SFTP server, or FTP server.

To discover the device to Junos Space Network Management Platform, you must download the configlet (with only the connection parameters or the complete configlet with the connection parameters and the device template configuration), copy the configlet to a USB drive, connect the USB drive to the device, and reboot the device.

The device connects to Junos Space Network Management Platform and is discovered to the Junos Space Network Management Platform database during the initial discovery process. For more

information about activating devices using configlets, see “Activating Devices by Using Configlets” on page 269.

- To activate the devices later, clear the **Activate Now** check box.

> **NOTE:** If you clear the Activate Now check box and choose to activate the device later, use the Activate Modeled Device workflow from the Device Management page to activate the device.

12. Click **Next**

    This page displays the devices that are to be modeled. By default, the devices are given the name you provided for the modeled instance appended with “_#,” where # is a number. The devices are numbered from 1 through the value you specified for the number of devices in this modeled instance.

    If you selected a static connection profile, enter the static IP address and gateway details on a per-device basis.

13. (Optional) Modify the default hostname, platform, IP address, and gateway details on a per-device basis.

14. Click **Finish**.

    The modeled instance is created. You are redirected to the Model Devices page.

    You can view the modeled devices that you created on the Device Management page.

> **NOTE:** To view the details of the modeled instance, select the modeled instance and select **View Modeled Instance** from the Actions menu.

RELATED DOCUMENTATION

- Model Devices Overview | **251**
- Adding More Devices to an Existing Modeled Instance | **274**
- Downloading a Configlet | **266**
- Viewing and Copying Configlet Data | **268**

Activating a Modeled or Cloned Device in Junos Space Network Management Platform

You activate a modeled device to manage the device in Junos Space Network Management Platform. The devices you activate through this workflow are ones that were created without selecting the Activate Now option. You can also use this workflow to activate a cloned device (created using the Clone Device workflow).

> **NOTE:** If you associated a device template to the modeled instance when creating the modeled instance, you must approve the device template configuration on the device by using the Review/Deploy Configuration workflow. The Activate Modeled Device task is disabled if you do not approve the device template configuration. For more information about reviewing and deploying the configuration to a device, see "Reviewing and Deploying the Device Configuration" on page 327.
>
> Ensure that the **Enable approval workflow for configuration deployment** check box on the Modify Application Settings page is selected to enable you to approve the configuration in the device template to the device. You cannot validate the configuration on a modeled device before deploying the configuration.

You can activate modeled devices by using the following methods:

- Junos Space–initiated connection – For this method, you need to specify the IP address and credentials of the device to connect to a device. If the Junos Space server can access the device, the device is discovered on Junos Space Platform.

  If you choose to deploy the configuration in the device template by using the Automatic or Manual option through a Junos Space-initiated connection, the device template is deployed to the device after the device is discovered to Junos Space Platform.

- Device-initiated connection – Use this method if the Junos Space server cannot access the device. This method involves copying the configlets from Junos Space Platform to the device. The device stays in the Waiting for Deployment state until the configlets are copied to the device. Then the device connects to and is discovered on Junos Space Platform during the initial discovery process.

  If you choose to deploy the configuration in the device template by using the Automatic option through a device-initiated connection, you must download the connection configlet from the Download Configlet page, copy the configlet to a USB drive, connect the USB drive to the device, and reboot the device. The device template is deployed to the device after the device is discovered to Junos Space Platform.

  If you choose to deploy the configuration in the device template by using the Manual option through a device-initiated connection, you must download the complete configlet (with the connection parameters and the device template configuration) from the Download Configlet page, copy the configlet to a USB

drive, connect the USB drive to the device, and reboot the device. The device template configuration is committed to the device when the device reboots.

> **NOTE:** The Download Configlet link is not available in the job details of a Junos Space–initiated connection.

To activate a modeled or cloned device in Junos Space Platform:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page that appears displays a list of devices that exist in the Junos Space Platform database.

2. Right-click the modeled or cloned device and select **Device Operations > Activate Modeled Device**.

   The Activate Modeled Device page is displayed.

3. Select whether you want to connect the device to Junos Space Platform by using a Junos Space–initiated connection or a device-initiated connection.

   By default, the Space initiated option button is selected.

   - To connect the device by using a device-initiated connection:

     a. Select the **Device Initiated** option button.

        The fields related to the device-initiated connection are displayed.

     b. (Optional) From the **Connection Profile** drop-down list, select a connection profile that specifies the connectivity parameters that you want to use for this device.

     c. (Optional) If you have not created a connection profile or want to create a new connection profile for this device, click the **Create** button next to the Connection Profile drop-down list.

        The Connection Profile pop-up window is displayed. For more information about creating a connection profile, see “Creating a Connection Profile” on page 252.

     d. In the **Username** field, enter the username used to manage the device.

        The username can contain 2 through 64 alphanumeric characters. The special characters allowed are hyphen (-) and underscore (_). The username must start with a nonhyphen character.

     e. (Optional) Select the **Key Based Authentication** check box to use RSA keys for authentication.

        By default, this check box is not selected.

     f. In the **Password** field, enter the password.

The maximum length is 20 characters, the minimum length is 6 characters, and all characters are allowed.

g. In the **Confirm Password** field, reenter the password used to manage the device.

h. (Optional) Select the **Serial Number Validation** check box to authenticate the device by using the serial number of the device.

By default, this check box is not selected.

If you select the Serial Number Validation check box, in the **Serial Number** field, enter the serial number of the device.

i. Select whether you want to deploy the initial configuration to the device during the initial connection to Junos Space Platform, or manually after the device is added. The **Device Configuration Update** options are **Automatic** and **Manual**.

- If you choose **Automatic**, the configuration is deployed to the device when the device is discovered to Junos Space Platform.

  This option is enabled by default.

- If you choose **Manual**, you must load the complete configlet, which includes the updated device configuration, through a USB device, SFTP server, or FTP server.

- To connect the device to Junos Space Platform by using a Junos Space–initiated connection:

a. Select the **Space Initiated** option button.

The fields related to Junos Space–initiated connection are displayed.

b. Select whether you want to specify a hostname or IP address for the device by using the **Toggle IP Address/HostName** check box.

By default, this check box is not selected and you can specify the IP address in the next field. If you select this check box, you can enter the hostname in the next field.

c. In the **IP Address** or **Hostname** field, enter the IP address or hostname of the device.

> **NOTE:** You can enter the IP address in either IPv4 or IPv6 format. Refer to http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml for the list of restricted IPv6 addresses.

d. In the **Username** field, enter the username used to manage the device.

The username can contain 2 through 64 alphanumeric characters. The special characters allowed are hyphen (-) and underscore (_). The username must start with a nonhyphen character.

e. (Optional) Select the **Key Based Authentication** check box to use RSA keys for authentication.

   By default, this check box is not selected.

f. In the **Password** field, enter the password used to manage the device.

   The maximum length is 20 characters, the minimum length is 6 characters, and all characters are allowed.

g. In the **Confirm Password** field, reenter the password.

h. To authorize a different user on the device during the activation process, select the **Authorize user on different device** check box.

   By default, this check box is not selected. If you select this check box:

   - In the **Username** field, enter the username used to manage the device.

     The username can contain 2 through 64 alphanumeric characters. The special characters allowed are hyphen (-) and underscore (_). The username must start with a nonhyphen character.

   - Select the **Key Based Authentication** check box to use RSA keys for authentication.

     By default, this check box is not selected.

   - In the **Password** field, enter the password used to manage the device.

     The maximum length is 20 characters, the minimum length is 6 characters, and all characters are allowed.

   - In the **Confirm Password** field, reenter the password.

     NOTE: If the user does not exist on the device, a new user is created with these credentials.

i. Select the **Serial Number Validation** check box if you want to authenticate the device by using the serial number of the device.

   By default, this check box is not selected.

   (Optional) The Serial Number field is displayed if you select the Serial Number Validation check box.

   If you select the Serial Number Validation check box, in the **Serial Number** field, enter the serial number of the device.

j. Select whether you want to deploy the initial configuration to the device during the initial connection to Junos Space Platform, or manually after the device is added to Junos Space Platform. The **Device Configuration Update** options are **Automatic** and **Manual**.

   - If you choose **Automatic**, the configuration is deployed to the device when the device is discovered to Junos Space Platform.

This option is enabled by default.

- If you choose **Manual**, you must load the complete configlet, which includes the updated device configuration, through a USB device, SFTP server, or FTP server.

4. Click **Activate**.

   A job is triggered. If you activated the device through a Junos Space–initiated connection, the job triggered does not contain the Download Configlet link. If the job succeeds, the device is flagged with either the Out of Sync or In Sync status on the Device Management page.

   If you activated the device through a device-initiated connection, the job triggered displays the Download Configlet link. The configlet is available on the Job Management page and the contents of the configlet vary depending on whether you selected the Automatic or Manual option to update the device template configuration. If the job succeeds, the device is flagged with the In Sync status on the Device Management page.

RELATED DOCUMENTATION

Model Devices Overview | 251

Creating a Modeled Instance | 257

Downloading a Configlet

You download a configlet to save a copy of the configlet on your local computer and connect devices to Junos Space Platform. You can download a configlet in XML, CLI, and curly braces formats. You download a configlet from the Devices workspace. Ensure that you temporarily disable the pop-blocker on your browser to be able to download the configlet file on your local computer.

This task is disabled if the modeled device is in the In Sync or Modeled state on the Device Management page.

NOTE: If you created a modeled device without using the Activate Now option when creating the modeled instance, you can download the configlet only from the Device Management page. To download the configlet from the Device Management page, select the modeled device and select **Device Operations > View/Download Configlet** from the Actions menu.

To download a configlet from the Model Devices page:

1. On the Network Management Platform user interface, select **Devices > Model Devices**.

   The Model Devices page is displayed.

2. Select the modeled instance whose configlet you want to download and select **Download Configlet** from the Actions menu.

   The Download Configlet page is displayed.

3. From the **Configlet Type** drop-down list, select the format of the configlet you want to download.

   You can download the configlet in CLI, XML, and curly braces formats.

4. Select whether you want to encrypt the configlet file by selecting the appropriate option button in the Encryption area.

   Junos Space Network Management Platform supports encrypting configlets in the AES format.

   - To use plain-text, select the **Plain Text** option button.
   - To use AES encryption, select the **AES** option button and enter the encryption key in the **Encryption Key** field.

     The encryption key must be 16 characters long and can contain letters, numbers, spaces, and special characters.

5. Select how you want to save or copy the configlet file by choosing the appropriate option button in the **Save** area.

   - If you select the **None** option button, the configlet file is saved on your local computer.
   - If you select the **SFTP** option button, specify the user ID, password, SFTP server IP address, and the file path where you want to save the configlet file on the SFTP server.
   - If you select the **FTP** option button, specify the user ID, password, FTP server IP address, and the file path where you want to save the configlet file on the FTP server.

6. Click **Download**.

7. Save the **Configlets.zip** file to your local computer if you want to save it locally.

NOTE: To connect and activate a modeled device from Junos Space Platform, download the configlet in any format, connect a USB device containing the configlet to the device, and reboot the device. The device then connects to Junos Space Platform. For more information, see "Activating Devices by Using Configlets" on page 269.

RELATED DOCUMENTATION

Model Devices Overview | 251

Creating a Modeled Instance | 257

Adding More Devices to an Existing Modeled Instance | 274

Viewing and Copying Configlet Data | 268

Viewing and Copying Configlet Data

You can view configlet data for the modeled instance that you created. You can also copy the configlet data to a text editor for further modifications.

This task is disabled if the modeled device is in the Managed state on the Device Management page or for a modeled device that is activated using a Junos Space–initiated connection.

> **NOTE:** If you created a modeled device without using the Activate Now option when creating the modeled instance, you can download the configlet only from the Device Management page. To view the configlet from the Device Management page, select the modeled device and select **Device Operations > View/Download Configlet** from the Actions menu.

To view and copy configlet data:

1. From the Junos Space Network Management Platform user interface, select **Devices > Model Devices**.

   The Model Devices page is displayed.

2. Select the modeled instance whose configlet data you want to view and copy, and select **View Configlet** from the Actions menu.

   The View Configlet page is displayed. You can view the name of the modeled instance, number of devices that are part of this modeled instance, and configlet data.

3. From the **Configlet Format** drop-down list, select the format in which you want to view the configlet data.

   The options available are CLI, XML, and curly braces. By default CLI is selected.

   > **NOTE:** If you activate a modeled device by using the Activate Now option when creating a modeled instance, you can download the configlet in CLI, XML, and curly brace formats.

4. Copy the configlet data from the Configlet Content field to a Notepad or any other text editor.

   If you select to update the configuration in the device template manually, the Configlet Content area displays the configlet containing the connection parameters and the configuration in the device template.

   You can modify this configlet as needed and copy the modified data in the configlet to a device's CLI console. The device then connects to Junos Space Platform.

5. Click **Close**.

   You are redirected to the Model Devices page.

RELATED DOCUMENTATION

- Model Devices Overview | **251**
- Creating a Modeled Instance | **257**
- Adding More Devices to an Existing Modeled Instance | **274**
- Downloading a Configlet | **266**

Activating Devices by Using Configlets

IN THIS SECTION

- Activating a Device by Using a Plain-text Single Configlet | **270**
- Activating a Device by Using an AES-encrypted Single Configlet | **270**
- Activating a Device by Using a Plain-text Bulk Configlet | **271**
- Activating a Device by Using an AES-encrypted Bulk Configlet | **271**

You can activate a modeled device by connecting a USB device containing the configlet generated from the appropriate modeled instance created in Junos Space Network Management Platform. The device then connects to Junos Space Platform through a device-initiated connection. Refer to"Activating a Modeled or Cloned Device in Junos Space Network Management Platform" on page 262 for more information.

You can generate a single configlet (per device) or a bulk configlet (one configlet to activate multiple devices).

- Junos Space Platform generates a single configlet if you choose a static connection profile or enable hostname validation and are using a DHCP connection profile.
- Junos Space Platform generates a bulk configlet if you do not select a connection profile or if you select a DHCP connection profile without hostname validation.

> **NOTE:** If you assigned a device template and selected to deploy the configuration in the device template manually, the configlet contains the connection parameters and the configuration in the device template.

By default, the configlet is downloaded as a .ZIP file in XML, CLI, or curly braces format. You must unzip the .ZIP file and copy the configlet to the USB device before using the configlet to activate devices.

The following tasks help you to activate modeled devices by using single or bulk configlets:

Activating a Device by Using a Plain-text Single Configlet

A plain text single configlet can be used to activate one device without an encryption key.

To activate a device by using a plain-text single configlet:

1. Copy the plain-text configlet to a USB device.
2. Plug the USB device to the USB port on the device.
3. Power on the device or reboot the device if the device was already powered on.

The configuration in the plain-text single configlet is committed on the device. The device then connects to Junos Space Platform.

Activating a Device by Using an AES-encrypted Single Configlet

An AES-encrypted single configlet can be used to activate one device with an the encryption key.

To activate a device by using an AES-encrypted single configlet:

1. Copy the AES-encrypted configlet to a USB device.
2. Create a text file **Key.txt** containing a 16-digit encryption key on the USB device.

3. Plug the USB device to the USB port on the device.

4. Power on the device or reboot the device if the device was already powered on.

   If you did not create the **Key.txt** file on the USB device, you are prompted to enter the 16-digit encryption key.

   - Enter the 16-digit encryption key.

The configuration in the AES-encrypted single configlet is committed on the device. The device then connects to Junos Space Platform.

Activating a Device by Using a Plain-text Bulk Configlet

A plain-text bulk configlet can be used to activate multiple devices without an encryption key.

To activate devices by using a plain-text bulk configlet:

1. Copy the plain-text bulk configlet to a USB device.

2. Create a text file **Hostname.txt** containing the hostnames of all devices that should be activated by this configlet, on the USB device.

3. Plug the USB device to the USB port on the device.

4. Power on the device or reboot the device if the device was already powered on.

The configuration in the plain-text bulk configlet is committed on the device. The device then connects to Junos Space Platform.

> **NOTE:** Repeat steps 1 through 4 to activate other devices using the same configlet.

Activating a Device by Using an AES-encrypted Bulk Configlet

An AES-encrypted bulk configlet can be used to activate multiple devices with an encryption key.

To activate devices by using an AES-encrypted bulk configlet:

1. Copy the AES-encrypted bulk configlet to a USB device.

2. Create a text file **Key.txt** containing a 16-digit encryption key on the USB device.

3. Create a text file **Hostname.txt** containing the hostnames of all devices that should be activated by this configlet, on the USB device.

4. Plug the USB device to the USB port on the device.

5. Power on the device or reboot the device if the device was already powered on.

   If you did not create the **Key.txt** file on the USB device, you are prompted to enter the 16-digit encryption key.

   - Enter the 16-digit encryption key.

The configuration in the AES-encrypted bulk configlet is committed on the device. The device then connects to Junos Space Platform.

> **NOTE:** Repeat steps 1 through 4 to activate other devices by using the same configlet.

RELATED DOCUMENTATION

- Rapid Deployment Overview | 247
- Creating a Modeled Instance | 257
- Viewing and Copying Configlet Data | 268

Viewing a Modeled Instance

You view a modeled instance when you need to view the details of a modeled instance.

To view a modeled instance:

1. On the Network Management Platform user interface, select **Devices > Model Devices**.

   The Modeled Devices page that appears displays the modeled instances.

2. Select the modeled instance you want to view and select the **View Modeled Instance** icon from the Actions bar.

   The View Modeled Instance dialog box is displayed.

   Table 22 lists the details of the modeled instance displayed in the View Modeled Instance dialog box.

Table 22: View Modeled Instance Dialog Box Details

Field	Description	Displayed In
Name	Name of the modeled instance	Model Devices page View Modeled Instance dialog box
Description	Description of the modeled instance	Model Devices page View Modeled Instance dialog box
Device Family	Device family used for the modeled instance	Model Devices page View Modeled Instance dialog box
Connection Profile Type	Type of connection profile used for the modeled instance	Model Devices page View Modeled Instance dialog box
Device Count	Number of devices in the modeled instance	Model Devices page View Modeled Instance dialog box

Table 23 lists the details of the devices included in the modeled instance.

Table 23: Details of Devices Included in the Modeled Instance

Field	Description
Device Name	Name of the modeled device
Platform	Platform of the modeled device
OS version	Junos OS version that is upgraded or downgraded on the modeled device
Serial Number	Serial number of the actual physical device
Static IP	Static IP address used during rapid deployment. A hyphen '-' is displayed if DHCP or PPPoE is used to assign IP addresses.

3. Click **Close** to close the View Modeled Instance dialog box.

RELATED DOCUMENTATION

Adding More Devices to an Existing Modeled Instance | 274
Viewing the Status of Modeled Devices | 275
Creating a Modeled Instance | 257
Deleting Modeled Instances | 276
Model Devices Overview | 251

Adding More Devices to an Existing Modeled Instance

You add more devices to an existing modeled instance if you want to add devices using the existing parameters of the modeled instance. You can perform this task from the Devices workspace.

To add more devices to a modeled instance:

1. On the Network Management Platform user interface, select **Devices > Model Devices**.

   The Model Devices page is displayed.

2. Select the modeled instance to which you want to add more devices and select **Add More Devices** from the Actions menu.

   The Add More Devices page is displayed. You can view the name of the modeled instance, the device family of the modeled instance, the device template associated with the modeled instance, the device image associated with the modeled instance, and the number of devices that are already part of the modeled instance.

3. (Optional) In the **Apply Tag** field, enter a tag that you want to assign to this modeled instance.

4. In the **Number of Devices to add** field, use the up and down arrows to specify the number of devices that you want to add to this modeled instance.

   The default value is zero.

   The page is populated with as many rows as the number of devices that you specify in the Number of Devices field. The Hostname, Platform, and OS version columns are populated with default values. You can modify the default hostname, and the platform of the device. If you have selected the Serial Number Validation check box in the modeled instance, you need to enter the serial number of the device.

   - If you want to modify the hostname for a device, double-click the hostname of the corresponding device and enter the new hostname
   - If you want to modify the platform for the device, select the appropriate platform for corresponding device from the drop-down list.

- Click **Update**.

5. Click **Add**.

   The devices are added to the modeled instance.

RELATED DOCUMENTATION

- Model Devices Overview | 251
- Creating a Modeled Instance | 257
- Downloading a Configlet | 266
- Viewing and Copying Configlet Data | 268

Viewing the Status of Modeled Devices

You view the status of the devices you added using a modeled instance to view the connection status and managed status of the devices. You can view the status of the devices you added using a modeled instance, from the Devices workspace.

To view the status of the modeled devices added using a modeled instance:

1. On the Network Management Platform user interface, select **Devices > Model Devices**.

   The Model Devices page is displayed.

2. Select the modeled instance and select **View Modeled Device Status** from the Actions menu.

   The View Modeled Device Status page is displayed. This page displays the name of the devices, Junos OS version on the devices, device family, platform of the devices, IP address of the devices, whether the device is connected to Junos Space Network Management Platform, the managed status of the devices, and the serial number of the devices.

3. Click **Back** to return to the Model Devices page.

RELATED DOCUMENTATION

- Model Devices Overview | 251
- Creating a Modeled Instance | 257
- Adding More Devices to an Existing Modeled Instance | 274

Downloading a Configlet | 266
Viewing and Copying Configlet Data | 268

Deleting Modeled Instances

You delete modeled instances when you no longer need them to add devices to Junos Space Network Management Platform. You can delete modeled instances from the Devices workspace.

To delete modeled instances:

1. On the Network Management Platform user interface, select **Devices > Model Devices**.

   The Model Devices page is displayed.

2. Select the modeled instances you want to delete and select **Delete Modeled Instances** from the Actions menu.

   The Delete Modeled Instances pop-up window is displayed.

3. Click **Delete**.

   The modeled instances are deleted.

RELATED DOCUMENTATION

Model Devices Overview | 251
Creating a Modeled Instance | 257
Adding More Devices to an Existing Modeled Instance | 274
Viewing and Copying Configlet Data | 268

Viewing a Connection Profile

You view a connection profile when you need to view the details of the connection profile.

To view a connection profile:

1. On the Network Management Platform user interface, select **Devices > Model Devices > Connection Profiles**.

   The Connection Profiles page that appears displays the connection profiles.

2. Select the connection profile you want to view and select the **View Connection Profile** icon from the Actions bar.

   The View Connection Profile dialog box is displayed.

   Table 24 lists the details of the connection profile displayed in the View Connection Profile dialog box.

   Table 24: View Connection Profile Dialog Box Details

Field or Area	Description	Displayed In
Name	Name of the connection profile	Connection Profiles page View Connection Profile dialog box
Description	Description of the connection profile	Connection Profiles page View Connection Profile dialog box
Interface	Interface of the device on which the IP address will be configured	View Connection Profile dialog box
IP Address Type	Format of the IP address: IPv4 or IPv6	View Connection Profile dialog box
NAT area	IP address of the NAT server and the port used for network address translation	View Connection Profile dialog box
Connection Settings area	How the IP address is assigned to the device DHCP, Static, or PPPoE and the fields related to the type of connection used to assign the IP address For example, a DHCP-based connection profile displays fields such as Retransmission Attempts, Retransmission Interval, Server Address, and so on.	View Connection Profile dialog box

3. Click **Close** to close the View Connection Profile dialog box.

RELATED DOCUMENTATION

Modifying a Connection Profile | 278

Creating a Connection Profile | 252

Model Devices Overview | 251

Cloning a Connection Profile

You clone a connection profile when you want to quickly create a copy of an existing connection profile and modify its parameters including the name of the connection profile. You can clone a connection profile from the Devices workspace.

To clone a connection profile:

1. On the Network Management Platform user interface, select **Devices > Model Devices > Connection Profiles**.

   The Connection Profiles page is displayed.

2. Select the connection profile you want to clone and select **Clone Connection Profile** from the Actions menu.

   The Clone Connection Profile page is displayed.

3. Modify the parameters of the connection profile. You can modify all the parameters including the name of the connection profile.

4. Click **Clone**.

   A new connection profile is created.

RELATED DOCUMENTATION

Modifying a Connection Profile | 278

Creating a Connection Profile | 252

Modifying a Connection Profile

You modify a connection profile to change some of the connectivity-related parameters of devices such as device interface details, the NAT configuration details for Junos Space, the protocol used to assign IP addresses to devices. You can modify connection profiles from the Connection Profiles page in the Devices workspace.

To modify a connection profile:

1. On the Network Management Platform user interface, select **Devices > Model Devices > Connection Profiles**.

The Connection Profiles page is displayed.

2. Select the connection profile you want to modify and click the Modify Connection Profile icon on the Actions menu.

   The Modify Connection Profile page is displayed. You can modify all the fields on this page except the Name field.

3. Click **Modify**.

   The connection profile is modified..

RELATED DOCUMENTATION

Deleting Connection Profiles | 279
Creating a Connection Profile | 252

Deleting Connection Profiles

You delete a connection profile when you no longer need it to create modeled instances. You can delete connection profiles from the Devices workspace.

To delete connection profiles:

1. On the Network Management Platform user interface, select **Devices > Model Devices > Connection Profiles**.

   The Connection Profiles page is displayed.

2. Select the connection profile you want to delete and click the Delete Connection Profiles icon on the Actions menu.

   The Delete Connection Profiles pop-up window is displayed.

3. Click **Delete**.

   The connection profile is deleted.

RELATED DOCUMENTATION

Modifying a Connection Profile | 278

Creating a Connection Profile | 252

CHAPTER 11

Device Authentication in Junos Space

IN THIS CHAPTER

- Device Authentication in Junos Space Overview | 281
- Generating and Uploading Authentication Keys to Devices | 285
- Resolving Key Conflicts | 291
- Modifying the Authentication Mode on the Devices | 293
- Acknowledging SSH Fingerprints from Devices | 295

Device Authentication in Junos Space Overview

IN THIS SECTION

- Credentials-Based Device Authentication | 282
- Key-Based Device Authentication | 282
- SSH Fingerprint-Based Device Authentication | 283
- Supported Algorithms for Junos Space SSH | 284

Junos Space Network Management Platform can authenticate a device by using credentials (username and password), keys (which use public-key cryptographic principles), or the devices' SSH fingerprints. You can choose the authentication mode on the basis of the level of security needed for the managed devices. The authentication mode is displayed in the Authentication Status column on the Device Management page. You can also change the authentication mode.

The following sections describe the authentication modes in Junos Space Platform:

Credentials-Based Device Authentication

To configure credentials-based authentication on your Junos Space setup, you need to ensure that the device login credentials with administrative privileges are configured on the device. If the device is reachable and the credentials are authenticated, these credentials are stored in the Junos Space Platform database. Junos Space Platform connects to the device by using these credentials. If you have configured key-based authentication on your Junos Space setup, you need to enter only the username to access the device.

Key-Based Device Authentication

From Junos Space Network Management Platform Release 16.1R1 onward, Junos Space Platform supports 4096-bit Rivest-Shamir-Adleman (RSA) algorithm, Digital Signature Standard (DSS), and Elliptic Curve Digital Signature Algorithm (ECDSA) public-key cryptographic principles to authenticate devices running Junos OS through key-based authentication. Junos Space Platform continues to support the 2048-bit RSA algorithm. Key-based authentication is more secure than credentials-based authentication because the device credentials need not be stored in the Junos Space Platform database.

RSA is an asymmetric-key or public-key algorithm that uses two keys that are mathematically related. Junos Space Platform includes a default set of public and private key pairs. The public key can be uploaded to the managed devices. The private key is encrypted and stored on the system on which Junos Space Platform is installed. For additional security, we recommend that you generate your own public and private key pair with a passphrase. A passphrase protects the private key on the Junos Space server. Creating long passphrases can be more difficult to break by brute-force attacks than shorter passphrases. A passphrase helps to prevent an attacker from gaining control of your Junos Space setup and trying to log in to your managed network devices. If you generate a new pair of keys, the keys are automatically uploaded to all active devices (that is, devices whose connection status is Up) that use Junos Space key-based authentication.

From Junos Space Network Management Platform Release 16.1R1 onward, you can also upload custom private keys to the Junos Space server and authenticate devices without the need to upload keys to devices from Junos Space Platform. With the custom key-based authentication method, you upload a private key with a passphrase to the Junos Space server. The device is authenticated using the existing set of public keys on the device, the private key uploaded to the Junos Space server, and the appropriate public-key algorithm—that is, RSA, ECDSA, or DSS. This authentication method can be used to authenticate devices during device discovery and later during device management.

If the keys are modified, the devices become unreachable and the authentication status changes to Key Conflict. You can use the Resolve Key Conflicts workflow to manually trigger the process of uploading new keys to these devices. To authenticate the devices, you can choose to upload the new keys generated from Junos Space Platform or use custom keys. If Junos Space key-based or custom key-based authentication fails, credentials-based authentication is automatically triggered.

After key-based or custom key-based authentication is enabled, all further communication to the devices is through Junos Space key-based or custom key-based authentication, without passwords. You can also

change the authentication mode from credentials-based to key-based or custom key-based for managed devices. For more information, see “Modifying the Authentication Mode on the Devices” on page 293.

You need to ensure the following to use key-based authentication in Junos Space Platform:

- The authentication keys are generated in the Administration workspace. For more information about generating and uploading keys to the devices, see “Generating and Uploading Authentication Keys to Devices” on page 285. The job result indicates whether the keys were successfully uploaded to the devices. On a multinode setup, the authentication keys are made available on all existing cluster nodes. Authentication keys are also made available on any subsequent nodes added to the setup.
- The device’s administrator credentials and the name of the user who connects to the Junos Space Appliance to upload the keys to the device are available.

SSH Fingerprint-Based Device Authentication

To avoid man-in-the-middle attacks or proxy SSH connections between Junos Space Platform and a device, Junos Space Platform can store the SSH fingerprint of the device in the Junos Space Platform database and validate the fingerprint during subsequent connections with the device. A fingerprint is a sequence of 16 hexadecimal octets separated by colons. For example, c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:83. You can specify the fingerprint for Juniper Networks devices during device discovery and validate the fingerprint when the devices connect to Junos Space Platform for the first time. You can specify fingerprints for a maximum of 1024 devices simultaneously in the Device Discovery workflow. If you do not specify the fingerprint, Junos Space Platform obtains the fingerprint details when it connects to the device for the first time. For more information, see “Viewing Managed Devices” on page 194.

Junos Space Platform does not recognize an SSH fingerprint change on a device during an active open connection with the device. SSH fingerprint changes are recognized only when the device reconnects to Junos Space Platform. The Authentication Status column on the Device Management page displays any conflicts or unverified authentication statuses.

Conflicts between SSH fingerprints stored in the Junos Space Platform database and those on the device can be resolved manually from the Junos Space user interface. Alternatively, you can allow Junos Space Platform to automatically update any fingerprint changes. To allow Junos Space Platform to automatically update SSH fingerprints, disable the Manually Resolve Fingerprint Conflict check box on the Modify Application Settings page in the Administration workspace. If you enable this check box, the Authentication Status column displays Fingerprint Conflict if a device’s fingerprint changes. You need to manually resolve the fingerprint conflict. For more information, see “Acknowledging SSH Fingerprints from Devices” on page 295.

NOTE: Key-based and fingerprint-based authentication modes are not supported in ww Junos OS devices.

Junos Space Platform verifies that the fingerprint on the device matches that in the database when you perform the following tasks:

- Staging a script on a device
- Staging a device image on a device
- Deploying a device image on a device
- Activating a replacement device
- Executing a script on a device
- Connecting to a device by using SSH

If the fingerprint on the device does not match the fingerprint stored in the Junos Space Platform database, the connection to the device is dropped. The connection status is displayed as Down and the authentication status is displayed as Fingerprint Conflict on the Device Management page.

Supported Algorithms for Junos Space SSH

Table 25 lists the supported algorithms for Junos Space SSH:

Table 25: Supported Algorithms for Junos Space SSH

Algorithm Type	FIPS Devices	Non-FIPS Devices
Key exchange algorithms	ecdh-sha2-nistp256, ecdh-sha2-nistp384, diffie-hellman-group14-sha1	ecdh-sha2-nistp256, ecdh-sha2-nistp384, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1
Host key algorithms	ecdsa-sha2-nistp256, ecdsa-sha2-nistp384	ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ssh-rsa, ssh-dss
Encryption algorithms(client to server)	aes128-ctr, aes192-ctr, aes256-ctr, aes128-cbc, aes192-cbc, aes256-cbc	aes128-ctr, aes192-ctr, aes256-ctr, aes128-cbc, aes192-cbc, aes256-cbc, 3des-ctr, blowfish-cbc, 3des-cbc
Encryption algorithms(server to client)	aes128-ctr, aes192-ctr, aes256-ctr, aes128-cbc, aes192-cbc, aes256-cbc	aes128-ctr, aes192-ctr, aes256-ctr, aes128-cbc, aes192-cbc, aes256-cbc, 3des-ctr, blowfish-cbc, 3des-cbc

Table 25: Supported Algorithms for Junos Space SSH *(continued)*

Algorithm Type	FIPS Devices	Non-FIPS Devices
MAC algorithm	hmac-sha1-96, hmac-sha2-256, hmac-sha256@ssh.com	hmac-sha1-96, hmac-sha2-256, hmac-sha256@ssh.com, hmac-sha1, hmac-md5, hmac-md5-96, hmac-sha256
Compression algorithm	zlib@openssh.com	zlib@openssh.com, none, zlib

Release History Table

Release	Description
16.1R1	From Junos Space Network Management Platform Release 16.1R1 onward, Junos Space Platform supports 4096-bit Rivest-Shamir-Adleman (RSA) algorithm, Digital Signature Standard (DSS), and Elliptic Curve Digital Signature Algorithm (ECDSA) public-key cryptographic principles to authenticate devices running Junos OS through key-based authentication.
16.1R1	From Junos Space Network Management Platform Release 16.1R1 onward, you can also upload custom private keys to the Junos Space server and authenticate devices without the need to upload keys to devices from Junos Space Platform.

RELATED DOCUMENTATION

- Device Discovery Profiles Overview | **220**
- Generating and Uploading Authentication Keys to Devices | **285**
- Resolving Key Conflicts | **291**
- Modifying the Authentication Mode on the Devices | **293**

Generating and Uploading Authentication Keys to Devices

IN THIS SECTION

- Generating Authentication Keys | **286**
- Uploading Authentication Keys to Multiple Managed Devices for the First Time | **287**
- Uploading Authentication Keys to Managed Devices With a Key Conflict | **290**

Junos Space Network Management Platform can authenticate a device either by using credentials (username and password) or by keys. Junos Space Network Management Platform supports RSA, DSA, and ECDSA public-key cryptographic principles to perform key-based authentication. You can select a key size of 2048 or 4096 bits. Junos Space Platform includes a default set of public-private key pairs; the public key is uploaded to the device and the private key is stored on the Junos Space server.

> **NOTE:** If you generated a new set of keys, you can either upload the new keys to the devices or resolve key conflicts when the device is disconnected from Junos Space Platform. For more information about resolving key conflicts, refer to "Resolving Key Conflicts" on page 291.

The following tasks describe how to the generate keys in Junos Space Platform and upload the public keys to the devices:

Generating Authentication Keys

To generate a public/private key pair for authentication during login to network devices:

1. On the Junos Space Network Management Platform user interface, select **Administration > Fabric**.

   The Fabric page is displayed.

2. Click the Manage SSH Key icon on the Actions bar.

   The Key Generator pop-up window is displayed.

3. (Optional) In the **Passphrase** field, enter a passphrase to be used to protect the private key, which remains on the system running Junos Space Network Management Platform and is used during device login. The passphrase must have a minimum of five and a maximum of 40 characters. A long passphrase is harder to break by brute-force guessing. Space, Tab, and Backslash (\) characters are not allowed. Although not mandatory, it is recommended that you set a passphrase to prevent attackers from gaining control of your system and logging in to your managed network devices.

4. (Optional) Select the **Show Passphrase** check box to view the passphrase you entered.

5. From the Algorithm drop down list, select the key algorithm used to the generate the key.

   The options are RSA, DSA, and ECDSA. By default, RSA is selected.

6. From the Key Size drop down list, select the length of the key algorithm that is uploaded to the devices.

   The options are 2048 Bits and 4096 Bits. By default, 2048 Bits is selected.

7. (Optional) Schedule the Junos Space Network Management Platform to generate authentication keys at a later time or immediately.
   - To specify a later start date and time for key generation, select the **Schedule at a later time** check box.
   - To initiate key generation as soon as you click **Generate**, clear the **Schedule at a later time** check box (the default).

   > **NOTE:** The selected time in the scheduler corresponds to the Junos Space server time but uses the local time zone of the client computer.

8. Click **Generate**.

   The Manage SSH Key Job Information dialog box appears, displaying a job ID link for key generation. Click the link to determine whether the key is generated successfully.

> **NOTE:** If there are already scheduled report generation or configuration backup tasks when you change the SSH key, ensure that you update the new SSH Key on the SCP server.

Uploading Authentication Keys to Multiple Managed Devices for the First Time

To upload authentication keys to multiple managed devices for the first time:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Click the Upload Keys to Devices icon on the Actions bar.

   The Upload Keys to Devices pop-up window is displayed.

3. You can upload the keys to one device or multiple devices:

   To upload keys to a single device:

   a. Select the **Add Manually** option button.

      The Authentication Details section that appears displays the options related to manually uploading keys to a single device.

   b. Select the **IP Address** or **Hostname** option button.

      If you selected the IP Address option, enter the IP address of the device.

      > **NOTE:** You can enter the IP address in either IPv4 or IPv6 format.

      If you selected the Hostname option, enter the hostname of the device.

   c. In the **Device Admin** field, enter the appropriate username for that device.

   d. In the **Password** field, enter the password for that device.

   e. (Optional) To authorize a different user on the target device, select the **Authorize different user on device** check box and enter the username in the **User on Device** field.

      If the username you specify in the **User on Device** field does not exist on the device, a user with this username is created and the key is uploaded for this user. If the **User on Device** field is not specified, then the key is uploaded for the device administrator user on the device.

   f. Click **Next**.

      You are directed to the next page. This page displays the details of the device you entered—IP Address/Hostname, Device Admin, Password, and User on Device.

   g. Click **Finish** to upload keys to the device.

      The Job Information dialog box appears.

   h. (Optional) Click the Job ID in the Job Information dialog box to view job details for the upload of keys to the device.

The Job Management page appears. View the job details to know whether this job is successful.

To upload keys to multiple devices:

a. Select **Import From CSV**.

b. (Optional) To see a sample CSV file as a pattern for setting up your own CSV file, select **View Sample CSV**. A separate window appears, allowing you to open or download a sample CSV file.

   Refer to the sample CSV file for the format of entering the device name, IP address, device password, and a username on the device. If the username you specify in the User on Device column does not exist on the device, a user with this username is created and the key is uploaded for this user. If the user on device column is not specified, then the key is uploaded for the device administrator user on the device.

c. When you have a CSV file listing the managed devices and their data, select **Select a CSV To Upload**.

   The Select CSV File dialog box appears.

d. Click **Browse** to navigate to where the CSV file is located on the local file system. Make sure that you select a file that has a .csv extension.

e. Click **Upload** to upload the authentication keys to the device.

   An Information dialog box displays information about the total number of records that are uploaded and whether this operation is a success.

   Junos Space Network Management Platform displays the following error if you try to upload non-CSV file formats:
   Please select a valid CSV file with '.csv' extension.

f. Click **OK** in the information dialog box that appears.

   The green check mark adjacent to the **Select a CSV To Upload** field indicates that the file is successfully uploaded.

g. Click **Next**.

   You are directed to the next page. This page displays the details of the device you entered—IP Address/Hostname, Device Admin, Password, and User on Device.

h. Click **Finish**.

   The Job Information dialog box appears.

i. (Optional) Click the Job ID to view job details for the upload of keys to the device.

The Job Management page appears. View the job details to know whether this job is successful.

New keys generated on Junos Space Platform are automatically uploaded to all managed devices.

Uploading Authentication Keys to Managed Devices With a Key Conflict

To upload authentication keys to one or several managed devices with a key conflict manually:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Select the devices with a key conflict to which you want to upload authentication keys and click the Upload Keys to Devices icon on the Actions bar.

   The Upload Keys to Devices pop-up window is displayed. The IP address fields of the devices are prepopulated.

3. In the **Device Admin** field, enter the appropriate username for that device.

4. In the **Password** field, enter the password for that device.

5. Confirm the password by reentering it in the **Re-enter Password** field.

6. Select **Next** to provide details for the next device.

7. Select **Upload** to upload the authentication keys to the managed devices.
   The Upload Authentication Key dialog box displays a list of devices with their credentials for your verification.

NOTE: If you do not specify a username in the User Name field, the key is uploaded for the “user admin” user on the device. If the username you specify in the User Name field does not exist on the device, a user with this username is created and the key is uploaded for this user.

RELATED DOCUMENTATION

Device Authentication in Junos Space Overview | 281

Device Discovery Profiles Overview | 220
Resolving Key Conflicts | 291

Resolving Key Conflicts

Devices that use public key-based authentication (that is keys generated and uploaded from Junos Space Network Management Platform) connect to Junos Space Platform by using RSA, DSS, or ECDSA Key public-key algorithms. If a new public key is generated from the Administration workspace when the device is disconnected or down, the device is unable to reconnect to Junos Space Platform when it comes back up. The Authentication Status column on the Device Management page shows that the device is in the Key Conflict state.

You can use the Resolve Key Conflict workflow to resolve the key conflict, then provide the new public key or use a custom private key to authenticate the device.

To resolve key conflicts:

1. On the Junos Space Network Management Platform user interface, select **Devices** > **Device Management**.

   The Device Management page is displayed.

2. Select the devices that are in the Key Conflict state.

3. Right-click and select **Device Access** > **Resolve Key Conflict** from the Actions menu.

   The Resolve Key Conflict page that appears displays a list of devices with key conflict.

You can either upload the new keys generated from Junos Space Platform or use a custom key to resolve the key conflict.

- To upload a custom key to the Junos Space server:

  i. Select the **Use Custom Key** option button.

     The Resolve Key Conflict page appears.

  ii. (Optional) In the Passphrase field, enter the passphrase created when you generated the private key.

  iii. Click the **Browse** button next to the Private Key field to upload the private key for the managed devices.

  iv. In the Device Admin column, enter the administrator username for the devices listed in the corresponding cells.

  v. Click **Resolve**.

     The key conflicts are resolved and the devices are pushed to the Key Based state.

- To upload new keys:

  i. Select the **Use Space Key** option button.

     By default, this option button is selected.

     The Resolve Key Conflict page appears.

  ii. In the Device Admin column, enter the administrator username for the devices listed in the corresponding cells.

     If the user does not exist on the device, a new user with the username is created.

  iii. In the Password column, enter the administrator password in the corresponding cells.

  iv. Click **Resolve**.

     The key configlets are resolved and the devices are pushed to the Key Based state.

To cancel the workflow, click **Cancel**.

RELATED DOCUMENTATION

Device Authentication in Junos Space Overview | 281
Modifying the Authentication Mode on the Devices | 293
Generating and Uploading Authentication Keys to Devices | 285

Modifying the Authentication Mode on the Devices

Junos Space Network Management Platform supports RSA, DSS, and ECDSA keys for key-based authentication. Junos Space Platform automates the processes for creating and uploading the keys. It also tracks and reports the authentication status of each device in the Devices workspace.

You can use this workflow to modify credentials on multiple devices, or change the authentication mechanism from credentials based to Junos Space Platform key based, credentials -based to custom key based or Junos Space Platform key based to custom key-based.

To modify the authentication mode on the devices:

1. On the Junos Space Network Management Platform user interface, select **Network Management Platform > Devices** > **Device Management**.

   The Device Management page appears.

2. Select the devices for which you want to modify the authentication.

3. Select **Device Access** > **Modify Authentication** from the Actions menu.

The Modify Authentication pop-up window is displayed.

- To modify the existing credentials on the selected devices:

  i. In the **Username** field, enter the username of the device.

     If the user does not exist on the device, the user is automatically created.

  ii. In the **Password** field, enter the password of the device.

  iii. In the **Confirm Password** field, reenter the password.

  iv. Select the **Change on device** check box.

  v. Click **Modify**.

     A Job is created. You can view the status of this job in the Job Management workspace.

- To modify the authentication mode from Junos Space Platform key-based to custom key-based:

  i. Select the **Key Based** option button.

  ii. In the **Username** field, enter the username of the device.

     If the user does not exist on the device, the user is automatically created.

  iii. Select the **Use Space Key** option button.

  iv. Click **Modify**.

     A job is created and the public key is uploaded to devices. You can view the status of this job in the Job Management workspace.

- To modify the authentication mode from credentials based or Junos Space Platform key based to custom key based:

  i. Select the **Key Based** option button.

  ii. In the **Username** field, enter the username of the device.

     If the user does not exist on the device, the user is automatically created.

  iii. Select the **Use Custom Key** option button.

  iv. (Optional) In the Passphrase field, enter the passphrase created when you generated the private key.

v. Click the **Browse** button next to the Private Key field to upload the private key for the managed devices.

vi. Click **Modify**.

A job is created and the private key is uploaded to the Junos Space server. You can view the status of this job in the Job Management workspace.

Click **Cancel** to close the Modify Authentication pop-up window.

You are redirected to the Device Management page.

RELATED DOCUMENTATION

Device Authentication in Junos Space Overview | 281

Generating and Uploading Authentication Keys to Devices | 285

Acknowledging SSH Fingerprints from Devices

You trigger this workflow to acknowledge the SSH fingerprints received from devices or resolve any SSH fingerprint conflicts between the fingerprints stored in the Junos Space Platform database and that on the devices. This workflow is enabled only if the Authentication Status column on the Device Management page displays the following status: Credentials Based – Unverified, Key Based – Unverified, Key Conflict – Unverified, or Fingerprint Conflict. Otherwise, this workflow appears dimmed.

NOTE: To view the SSH fingerprint on the device, run the following command in shell:

ssh-keygen -E md5 -lf /etc/ssh/ssh_host_rsa_key.pub.

To acknowledge the SSH fingerprints from the devices:

1. On the Network Management Platform user interface, select **Network Management Platform > Devices > Device Management**.

   The Device Management page is displayed.

2. Select the devices whose fingerprints you want to acknowledge and select **Device Access > Acknowledge Device Fingerprint** from the Actions menu.

   The Acknowledge Device Fingerprint page is displayed. Table 26 lists the columns on this page.

Table 26: Acknowledge Device Fingerprint Page

Column name	Description
Host Name	Hostname of the device
IP Address	IP address of the device
Authentication Status	Authentication status of the device
Fingerprint	If the Authentication Status column displays Fingerprint Conflict, this column displays the current fingerprint value of the device as stored in the Junos Space Platform database. This column does not display any value if the Authentication Status column displays Key Conflict – Unverified, Key Based – Unverified, or Credentials Based - Unverified.
New Fingerprint	If the Authentication Status column displays Fingerprint Conflict, this column displays the new fingerprint value received from the device. This column displays the current fingerprint value of the device as stored in the Junos Space Platform database if the Authentication Status column displays Key Conflict – Unverified, Key Based – Unverified, or Credentials Based - Unverified. You can also edit this column.

3. You can accept the fingerprint value received from the devices or modify the values.

   - To accept the fingerprint values:

     i. Click **Verify**.

        The Acknowledge Device Fingerprint dialog box appears, displaying the job ID of this job.

     ii. Click **OK**.

        You are redirected to the Device Management page.

   - To modify the fingerprint value of a device with the authentication status as Fingerprint Conflict:

     i. Click the **New Fingerprint** column corresponding to the device.

     ii. Enter the new fingerprint value and click **Update**.

     iii. Click **Verify**.

        The Acknowledge Device Fingerprint dialog box appears, displaying the job ID of this job.

     iv. Click **OK**.

        You are redirected to the Device Management page.

   - To modify the fingerprint value of a device with the authentication status displayed as Key Conflict–Unverified, Key Based–Unverified, or Credentials Based–Unverified:

     i. Click the **New Fingerprint** column corresponding to the device.

     ii. Enter the new fingerprint value and click **Update**.

        The Confirm Acknowledge dialog box is displayed.

     iii. Click **OK**.

        The new fingerprint is updated in the Junos Space Platform database. The connection to the device is reset.

     iv. Click **Verify**.

        The Acknowledge Device Fingerprint dialog box appears, displaying the job ID of this job.

> **NOTE:** If you are acknowledging the SSH fingerprint of from a dual Routing Engine, Virtual Chassis, or an SRX Series cluster device, a pop-up window is displayed with the following message: **Duplicate fingerprint observed. This is permitted for dual RE, VC and SRX cluster devices. Do you want to continue?**. Click **OK**.

v. Click **OK**.

   You are redirected to the Device Management page.

When the job is complete, the authentication status of the device moves from the unverified or conflicted status to the normal status. An audit log entry is generated for this workflow.

(Optional) To cancel acknowledging the fingerprints, click **Cancel**.

The devices remain in their original authentication statuses if you cancel the workflow.

RELATED DOCUMENTATION

Device Authentication in Junos Space Overview | 281

Device Discovery Profiles Overview | 220

CHAPTER 12

Viewing Device Inventory

IN THIS CHAPTER

- Device Inventory Overview | 299
- Viewing the Physical Inventory | 301
- Displaying Service Contract and EOL Data in the Physical Inventory Table | 305
- Viewing Physical Interfaces of Devices | 306
- Viewing Logical Interfaces | 308
- Viewing and Acknowledging Inventory Changes on Devices | 309

Device Inventory Overview

IN THIS SECTION

- Inventory for Aggregation and Satellite Devices | 300

You manage the device inventory from the Devices workspace in Junos Space Network Management Platform. The inventory of a device in the Junos Space Platform database is generated and stored when the device is first discovered and synchronized with the Junos Space Platform database. After the synchronization, the device inventory in the Junos Space Platform database matches the inventory on the device.

If either the physical (hardware) or logical (configuration) inventory on the device is changed, then the inventory on the device is no longer synchronized with the inventory of the device in the Junos Space Platform database. However, Junos Space Platform automatically triggers a resynchronization job when a configuration change request commit or out-of-band CLI commit operation occurs on a managed device.

You can also manually resynchronize the Junos Space Platform database with the physical device by using the **Resynchronize with Network** workflow from the Devices workspace on the Junos Space Platform user interface.

If Junos Space Platform is the system of record, the database values have precedence over any out-of-band changes to the network device configuration, and neither manual nor automatic resynchronization is available.

You can perform the following tasks related to the device inventory from the Devices workspace:

- List the device inventory to view information about the hardware and software components of each device that Junos Space Platform manages.
- View and acknowledge the inventory changes on the devices.
- View information about the service contract or end-of-life status for a part.
- View the location and ship-to-address of a device if address groups are configured in Service Now.
- View the operational and administrative statuses of the physical interfaces of the devices.
- View the software and license inventory on the devices.
- Export the physical and software inventory for use in other applications, such as those used for asset management.
- View information about the scripts associated with or executed on the interfaces of devices.
- Troubleshoot problems on devices.
- If the network is the system of record, resynchronize the network devices managed by Junos Space Platform with the Junos Space Platform database.

Inventory for Aggregation and Satellite Devices

Starting with Junos Space Network Management Platform Release 15.2R1, you can discover and manage an MX Series router configured as an aggregation device in Junos Space Platform. You can view the physical inventory of both the aggregation and satellite devices, cascade ports on the aggregation device, Flexible PIC Concentrators (FPC) slots to which the satellite devices are mapped, and satellite software packages and software upgrade groups with which the satellite devices are associated. For more information about aggregation devices, satellite devices, and Junos Fusion technology, refer to the *Junos Fusion* documentation.

A Junos Fusion setup with an MX240 router connected to three satellite devices discovered on Junos Space Platform displays the following details on Junos Space Platform:

- Mode of the aggregation device and the number of satellite devices connected to the aggregation device on the Device Management page. For more information, refer to "Viewing Managed Devices" on page 194.
- Physical inventory on the View Physical Inventory page. View the physical inventory of satellite devices associated with the FPC slots and the satellite alias name of the satellite device. For example, FPC slot 100 is associated with a QFX5100 device and FPC slots 101 and 103 are each associated with two EX4300 switches. Satellite alias name of the QFX5100 device is qfx5100-48s-02 and EX4300 switches are ex4300-48s-02 and ex4300-48s-05.

- Cascade ports on the aggregation device and the management IP addresses of the satellite devices on the View Physical Interfaces page. For example, the MX240 router connects to QFX5100 through xe-0/0/2 and EX4300 switches through xe-2/0/0 and xe-0/0/3.
- Satellite software packages and software upgrade groups on the View Software Inventory page. For example, *grp_mojito* satellite software upgrade group associated with the *15.1-20151224_s4_linux_44.1.0* software package.

Release History Table

Release	Description
15.2R1	Starting with Junos Space Network Management Platform Release 15.2R1, you can discover and manage an MX Series router configured as an aggregation device in Junos Space Platform.

RELATED DOCUMENTATION

Device Management Overview | **189**

Understanding How Junos Space Automatically Resynchronizes Managed Devices | **216**

Resynchronizing Managed Devices with the Network | **448**

Viewing the Physical Inventory | **301**

Exporting the Physical Inventory of Devices | **318**

Exporting the License Inventory | **312**

Viewing the Physical Inventory

Junos Space Network Management Platform displays the physical inventory of a device containing data retrieved from the device during discovery and resynchronization operations and from the data stored in the hardware catalog. This inventory includes the number of available slots for managed devices, power supplies, chassis cards, fans, part numbers, and so on.

Sorting is disabled on the View Physical Inventory page to preserve the natural slot order of the devices.

NOTE:

- If you select a chassis cluster device, information about both the primary and secondary devices is displayed.
- If you select a device with dual Routing Engines, the inventory data collected from the primary Routing Engine is displayed.
- If you select an aggregation device, the inventory data from the aggregation device and the satellite devices is displayed.

To view the physical inventory:

1. On the Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page displays the devices managed by Junos Space Platform.

2. Select a device whose physical inventory you want to view.

3. Select **Device Inventory > View Physical Inventory** from the Actions menu. Alternatively, right-click the device name and select **Device Inventory > View Physical Inventory**.

   The View Physical Inventory page is displayed. You can expand certain categories (for example, the Routing Engine category) to view data for all memory (RAM and disk) installed on the device components.

   If you select multiple devices, expand the category next to each device to view the physical inventory of the device.

   Table 27 displays the columns on the View Physical Inventory page.

   Table 27: View Physical Inventory Page

Column	Description
Module	Type of module on the device
Device Name	Name of the device
Model Number	Model number of the component
Model	Model of the device
Part Number	Part number of the device
Vendor Part Number	Part number of the optical module installed on the device
Vendor Material Number	Material number of the optical module installed on the device

Table 27: View Physical Inventory Page *(continued)*

Column	Description
Revision	Revision number of the device
Serial Number	Serial number of the component
Status	Status of the component: Online or Offline. The status is updated during periodic resynchronization of configuration information and on notification.
Domain	Domain to which the device is assigned
Description	Description of the component

NOTE: The device inventory for a Junos Space Platform installation that contains Service Now and Service Insight includes columns related to service contracts and the end-of-life status. For detailed information, see "Displaying Service Contract and EOL Data in the Physical Inventory Table" on page 305.

The address group subtypes—namely, the location and ship-to-address of a device—are displayed as columns only if Service Now contains an address group and the managed devices are associated with the address group. If no address group is configured in Service Now, these columns are not displayed.

4. (Optional) To view all the physical inventory of a device, click the – (minus) icon next to a Flexible PIC Concentrator (FPC).

   The inventory associated with the FPC collapses to a concise view.

5. (Optional) To view the physical inventory of a satellite device connected to an aggregation device, click the + (plus) icon next to an FPC (range: 100–255).

   The inventory of the satellite device associated with the FPC is displayed.

6. (Optional) To view the physical interfaces of an inventory element, right-click and select **View Physical Interfaces**.

   The View Physical Interfaces page is displayed. The Table 28 table describes the information that can be viewed on the View Physical Interfaces page.

7. (Optional) To export the physical inventory on the View Physical Inventory page:

   a. Click the Export icon at the top-left corner of the page.

      The Export Inventory dialog box is displayed.

   b. You can cancel or proceed with the export operation.

      - To cancel the export operation, click **Cancel**.

      - Click **Export** to export the inventory.

        The Export Inventory Job Status information dialog box is displayed. When the job is completed, the Export Inventory Job Status report indicates that the job is complete.

   c. Click the **Download** link in the Export Inventory Job Status information dialog box to download the CSV file.

      The CSV file you have downloaded displays physical inventory such as the name of the device, chassis, name of the module, name of the sub-module, name of the sub-sub-module, name of the sub-sub-sub-module, model number of the device, model of the device, part number of the device, revision number of the device, serial number of the device, vendor part number, vendor material number, and the description provided for the device.

   d. Close the Export Inventory Job Status information dialog box to return to the View Physical Inventory page.

      NOTE: You can also export the physical inventory of one or multiple devices managed by Junos Space Platform from the Device Management page. For more information, refer to "Exporting the Physical Inventory of Devices" on page 318.

8. Click **Back** at the top left to return to the Device Management page.

RELATED DOCUMENTATION

Displaying Service Contract and EOL Data in the Physical Inventory Table | 305

Exporting the Physical Inventory of Devices | 318

Viewing Managed Devices | 194

Viewing Physical Interfaces of Devices | 306

Resynchronizing Managed Devices with the Network | 448

Exporting the License Inventory | 312

Understanding How Junos Space Automatically Resynchronizes Managed Devices | 216

Displaying Service Contract and EOL Data in the Physical Inventory Table

Problem

Description: As of Release 11.3 of Junos Space, the Physical Inventory table can include columns related to the part's service contract and end-of-life (EOL) status.

The service contract data in this table is populated by the Service Now Devices table. The EOL data in this table is populated by the Service Insight Exposure Analyzer table. If Service Now or Service Insight is not installed, or if the required tables are empty, these columns are not displayed in the Physical Inventory table.

Solution

To investigate missing service contract and EOL data:

1. Use the table column display filters to check whether the columns have been hidden.

   Select the columns you want. If the columns cannot be selected (are not listed), check your Service Now and Service Insight settings.

2. Check the Service Now Devices table for details about the devices managed with Junos Space Network Management Platform, including information about the service contract.

   If you are unable to view service contract information, check the Service Now settings to ensure the following items have been properly configured:

   - Service Now Organization. See Organizations Overview topic in the Service Now documentation.
   - Service Now Device. See Service Now Devices Overview topic in the Service Now documentation.
   - Service Now Device Group. See Associating Devices with a Device Group topic in the Service Now documentation.
   - Service Now Event Profile. See Event Profiles Overview topic in the Service Now documentation.

3. Check the Service Insight Exposure Analyzer table for details about the devices managed with Junos Space Network Management Platform, including information about EOL announcements.

The EOL Status column indicates whether EOL data is available or not. EOL data is available only if there is an EOL bulletin. EOL data is typically unavailable for newer products. If the Exposure Analyzer table does not contain records, there might be a problem with the Service Now configuration. Service Now manages the communication between Junos Space Network Management Platform and the Juniper Networks support organization, which is the originating source of EOL data. If the Service Insight Exposure Analyzer table is empty, check the following Service Now settings:

- Service Now Organization. See the Organizations Overview topic in the Service Now documentation.
- Service Now Device. See the Service Now Devices Overview topic in the Service Insight documentation.

RELATED DOCUMENTATION

Viewing the Physical Inventory | 301

Viewing Physical Interfaces of Devices

Junos Space Network Management Platform displays physical interfaces by device name, on the basis of the device information in the Junos Space Platform database. You can view the operational status and administrative status of physical interfaces for one or more devices to troubleshoot problems.

If the interface status changes on the managed device, the information is not updated in Junos Space Platform until the device is resynchronized with the Junos Space Platform database.

NOTE: You can view the physical interfaces of devices from the Device Management page. To view the physical interfaces of a device from the Device Management page, click the **View** link in the Physical Interfaces column corresponding to the device. You are redirected to the View Physical Interfaces page.

To view the physical interfaces of devices:

1. On the Network Management Platform user interface, select **Devices** > **Device Management**.

   The Device Management page displays the devices managed by Junos Space Platform.

2. Select the devices for which you want to view the physical interfaces and select **Device Inventory > View Physical Interfaces** from the Actions menu.

   Alternatively, right-click the names of the device and select **Device Inventory > View Physical Interfaces**.

The View Physical Interfaces page that appears displays the physical interfaces and the status of the physical interfaces of the device. Table 28 describes the information that is displayed on the View Physical Interfaces page.

Table 28: View Physical Interfaces Page

Column	Description
Device Name	Name of the device as stored in the Junos Space Platform database. This column is displayed by default.
Physical Interface Name	Standard information about the interface, in the *type-/fpc/pic/port* format, where *type* is the media type that identifies the network device; for example, ge-0/0/6.
IP Address	IP address of the interface
IPv6 Address	IPv6 address of the interface. The address is displayed only if an IPv6 address is configured on the device.
Logical Interfaces	Link to the table of logical interfaces of the device
MAC Address	MAC address of the device
Operational Status	Operational status of the interface: Up or Down
Admin Status	Administrative status of the interface: Up or Down
Link Level Type	Link level type of the physical interface
Link Type	Physical interface link type: full duplex or half duplex
Speed (Mbps)	Speed at which the interface is running
MTU	Maximum transmission unit size on the physical interface
Description	An optional description for this interface configured on the device. It can be any text string of 512 or fewer characters. Any longer string is truncated to 512 characters. If there is no information, the column is empty.
Domain	Domain to which the device is assigned

3. (Optional) Select the columns displayed on the View Physical Interfaces page by mousing over any column head and clicking Columns on the drop-down list, then selecting the check boxes against the names of the columns that should be displayed.

The selected columns are displayed on the View Physical Interfaces page.

4. Click **Back** on the top-left corner to return to the Device Management page.

RELATED DOCUMENTATION

Viewing Managed Devices | 194
Viewing the Physical Inventory | 301
Exporting the License Inventory | 312
Viewing Logical Interfaces | 308

Viewing Logical Interfaces

You can view logical interfaces on a per-port basis or on a per-device or per-logical system basis. You can view the logical interface configurations for one or more devices or logical systems to troubleshoot problems.

You can access the Logical Interfaces view in either of two ways: from the Manage Devices inventory page, or from within the Physical Interfaces view. These two procedures are described separately below.

To view the logical interfaces configured for a selected device from the Manage Devices inventory page:

1. On the Network Management Platform user interface, select **Devices > Device Management**.
   A tabular list of devices appears.

2. Select the devices for which you want to view logical interface information and select **Device Inventory > View Logical Interfaces** from the Actions menu.

   Junos Space Network Management Platform displays the status of the logical interfaces for the selected devices in a table. Its possible fields are described in Table 29. Some columns may be hidden. To expose them, mouse over any column head, click the down arrow that appears, select **Columns** from the resulting menu, and check the columns you want to see.

   Table 29: Logical Interfaces Columns

Column	Description
Device Name	Configuration name of the device. This column is displayed by default.
Interface Name	Standard information about the interface, in the format *type-/fpc/pic/port/logical interface*, where *type* is the media type that identifies the network device; for example, ge-0/0/6.135.

Table 29: Logical Interfaces Columns *(continued)*

Column	Description
IP Address	IP address for the logical interface
IPv6 Address	IPv6 address for the interface. The address is displayed only if an IPv6 address is configured on the device.
Encapsulation	Encapsulation type used on the logical interface
Vlan	VLAN ID for the logical interface
Description	An optional description configured for the interface. It can be any text string of 512 or fewer characters. Any longer string is truncated. If there is no information, the column entry is blank.
Domain	Domain to which the device is assigned

3. Select **Return to Inventory View** at the top left of the display.

RELATED DOCUMENTATION

Viewing Physical Interfaces of Devices | 306

Viewing and Acknowledging Inventory Changes on Devices

You can view the list of inventory changes performed on the devices that are managed on Junos Space Network Management Platform. You can also acknowledge the inventory changes on the devices.

To view and acknowledge the list of inventory changes on devices:

1. On the Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page that appears displays the list of devices managed on Junos Space Platform.

2. Right-click the devices whose inventory changes you need to view or acknowledge and select **Device Inventory > View/Acknowledge Inventory Changes**.

   The View Inventory Changes page is displayed.

> **NOTE:** The **View/Acknowledge Inventory Changes** task is disabled if there are no pending and acknowledged inventory changes.

This page displays two tabs: Inventory Changes and Acknowledged Inventory Changes. By default, the Inventory Changes tab is displayed.

Table 30 describes the columns displayed on the Inventory Changes tab.

Table 30: Inventory Changes Tab

Column Name	Description
Id	ID of the inventory change
Device Name	Name of the device
Component Name	Name of the component on the device
Path	XPath of the component on the device
Serial Number	Serial number of the device
Part Number	Part number of the device
Operation	Type of inventory change performed: Added or Removed.
Date Time	Time at which the component was removed from or added to the device

3. To view the acknowledged inventory changes, select the **Acknowledged Inventory Changes** tab.

   This tab displays the same columns as on the Inventory Changes tab and an additional column User. The User column specifies the username of the user who acknowledged the inventory change.

4. To acknowledge the inventory changes, select the **Inventory Changes** tab.

5. Select the inventory changes you need to acknowledge and click the Acknowledge icon on the tool bar.

   The Inventory Changes information dialog box is displayed.

6. Click **OK** to confirm the inventory changes.

   The inventory changes are acknowledged.

RELATED DOCUMENTATION

Viewing the Physical Inventory | 301

Viewing Managed Devices | 194

CHAPTER 13

Exporting Device Inventory

IN THIS CHAPTER

- Exporting the License Inventory | 312
- Viewing and Exporting the Software Inventory of Managed Devices | 316
- Exporting the Physical Inventory of Devices | 318

Exporting the License Inventory

The Device Licence Inventory feature enables you to display the currently installed license inventory information for all DMI schema-based devices under Junos Space Network Management Platform management.

The license inventory is generated when the device is first discovered and synchronized in Junos Space Network Management Platform.

The licenses used by all Juniper Networks devices are based on SKUs, which represent lists of features. Each license includes a list of features that the license enables and information about those features. Sometimes the license information also includes the inventory keys of hardware or software elements upon which the license can be installed.

> **NOTE:** To view the license(s) for Junos Space Network Management Platform itself, see "Viewing Junos Space Licenses" on page 1326.

This topic also covers:

- Absence of license
- Trial information
- Count-down information
- Date-based information

DMI enables each device family to maintain its own license catalog in the DMI Update Repository. The license catalog is a flat list of all the licenses used by a device family. The key for a license element is its SKU name. Each license element in the catalog includes a list of features that the license enables and information about each feature (that is, its name and value). Optionally, the license element can also list the inventory keys of hardware or software elements and where it can be installed.

If the license inventory on the device is changed, the result depends on whether the network is the system of record or Junos Space Network Management Platform is the system of record. See "Systems of Record in Junos Space Overview" on page 214.

If the network is the system of record, Junos Space Network Management Platform automatically synchronizes with the managed device. You can also manually resynchronize the Junos Space Network Management Platform license database with the device by using the Resynchronize with Network action. See "Resynchronizing Managed Devices with the Network" on page 448.

If Junos Space Network Management Platform is the system of record, neither automatic nor manual resynchronization is available.

Viewing device license inventory does not include pushing license keys to devices. You can, however, push licenses with the Configuration Editor to any device that has license keys in its configuration. You can export device license inventory information to a CSV file for use in other applications.

License inventory information shows individually installed licenses as well as a license usage summary, with statistics for various features.

To export the license inventory for a device:

1. On the Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page displays the devices managed in Junos Space Network Management Platform.

2. Select **Device Inventory > View License Inventory** from the Actions menu.

   The License Inventory page displays the license information listed in Table 31.

   > **NOTE:** Need Counts in red indicate violations. In other words, entries in red indicate that you are using features that you are not licensed to use. You may also encounter the message that you have no licenses installed.

3. (Optional) View the list of licensed features for the selected license by double-clicking a license usage summary or clicking on the forward action icon to the left of a license usage summary.

   The information displayed is described in Table 32.

4. (Optional) Click **Return to Inventory View** at the top of the inventory page.

5. (Optional) Click **Export** at the top of the inventory page, to export the license inventory information.

   The Export Device License Information dialog box appears, displaying a link: Download license file for selected device (CSV format).

6. (Optional) Click the download link.

   The Opening Device License-*xxxxxx*CSV dialog box appears, where *xxxxxx* represents a number.

7. Open the file with an application of your choice, or download the file by clicking **Save**.

   The CSV file contains the fields described in Table 32 and Table 33. These fields are not populated if the information is not available for the selected license.

> **NOTE:** Exporting device license information generates an audit log entry.

Table 31: License Usage Summary Fields

Field	Description
Feature name	Name of the licensed SKU or feature. It can be used to look up the license with Juniper Networks. Not all devices support this.
License count	Number of times an item has been licensed. This value may have contributions from more than one licensed SKU or feature. Alternatively, it may be 1, no matter how many times it has been licensed.
Used count	Number of times the feature is used. For some types of licenses, the license count will be 1, no matter how many times it is used. For capacity-based licensable items, if infringement is supported, the license count may exceed the given count, which has a corresponding effect on the need count.
Need count	Number of times the feature is used without a license. Not all devices can provide this information.
Given count	Number of instances of the feature that are provided by default.

Table 32: License Feature or SKU Fields

Field	Description
Feature Name	Name of the licensed SKU or feature. It can be used to look up the license with Juniper Networks. Not all devices support this.
Validity Type	The SKU or feature is considered permanent if it is not trial, count-down, or data-based.

Table 33: Additional Fields in CSV Files

Field	Description
State	Status of the license: valid, invalid, or expired. Only licenses marked as valid are considered when calculating the license count.
Version	Version of the license.
Type	Permanent, trial, and so on.
Start Date	Licensed feature starting date.
End Date	Licensed feature ending date.
Time Remaining	Licensed feature time remaining.

RELATED DOCUMENTATION

- Viewing Managed Devices | 194
- Resynchronizing Managed Devices with the Network | 448
- Understanding How Junos Space Automatically Resynchronizes Managed Devices | 216
- Systems of Record in Junos Space Overview | 214

Viewing and Exporting the Software Inventory of Managed Devices

Junos Space Network Management Platform displays a list of currently installed software inventory for all DMI schema–based managed devices. The software inventory information is generated when the device is first discovered and synchronized with the Junos Space Platform database. You can also update the software inventory information, if the software inventory on the device is changed by a local user, by synchronizing the device with the Junos Space Platform database. The synchronization with the database depends on whether the network or Junos Space Platform is the system of record.

If the network is the system of record, Junos Space Platform database is automatically synchronized. You can also manually resynchronize the Junos Space Platform software database with the device by using the Resynchronize with Network action. For more information, refer to "Resynchronizing Managed Devices with the Network" on page 448.

If Junos Space Platform is the system of record, neither automatic nor manual resynchronization is available. You can reset the device configuration from the values in the Junos Space Platform database if and when you want to do so. For more information, refer to "Systems of Record in Junos Space Overview" on page 214.

You can export device software inventory to a CSV file, which can be used in other applications.

> **NOTE:** Juniper Networks devices require a license to activate the feature. To understand more about Junos Space Network Management Platform Licenses, see, Licenses for Network Management. Please refer to the Licensing Guide for general information about License Management. Please refer to the product Data Sheets for further details, or contact your Juniper Account Team or Juniper Partner.

To view the software inventory of devices:

1. On the Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page displays the devices managed in Junos Space Platform.

2. Select the devices and select **Device Inventory > View Software Inventory** from the Actions menu.

   The View Software Inventory page is displayed with a list of the software on the devices.

   Table 34 displays the columns on the View Software Inventory page.

   Table 34: View Software Inventory Page

Field	Description
Device Name	Name of the device as stored in the Junos Space Platform database

Table 34: View Software Inventory Page *(continued)*

Field	Description
Model	Model of this device: J Series, M Series, MX Series, TX Series, SRX Series, EX Series, BXOS Series, and QFX Series
Routing engine	On a device supporting multiple Routing Engines, indicates which Routing Engine is used
Package name	Name of the installed software package For an aggregation device, this column also displays the satellite software upgrade groups created on the aggregation device. If you installed a satellite software package on the satellite device during the autoconversion procedure (without adding the device to a satellite software upgrade group) and did not upgrade the satellite software package, this column displays the base satellite software package.
Description	Description of the installed software package
Version	Version number of the installed software package For an aggregation device, this column also displays the satellite software package associated with the corresponding satellite software upgrade group.
Type	Type of the installed software package: Operating System, Internal Package, or Extension
Major	Major portion of the version number. For example, in version 15.1R2, the major portion is 15.
Minor	Minor portion of the version number. For example, in version 15.1R2, the minor portion is 1.
Revision number	Revision number of the package. For example, in version 15.1R2, the revision number is 2.

3. If you selected more than one device, the View Software Inventory page is grouped by device name. To expand or contract the software inventory of a device, click the icon to the left of the device name.

   The complete software inventory of a device are displayed.

4. (Optional) Sort the columns on the View Software Inventory page either by clicking the arrow in the column head or by mousing over the column head and clicking Sort Ascending or Sort Descending.

   The columns on the View Software Inventory page are sorted.

5. (Optional) Select the columns displayed on the View Software Inventory page by mousing over any column head and selecting Columns from the drop-down list, then selecting the check boxes against the names of the columns that should be displayed.

   The selected columns are displayed on the View Software Inventory page.

   The Version column is redundant against the Major, Minor, and Revision columns.

6. (Optional) To export the software inventory information:

   a. Click the Export icon at the top of the inventory page.

      The Export Software Inventory dialog box appears, displaying a link: Download software inventory for selected device (CSV format).

   b. Click the **Download** link.

   c. Open the file with an application of your choice, or download the file by clicking **Save**. You can designate a filename and location.

      The CSV file contains the following fields: Device Name, Product Model, Package Name, Version, Type, and Description, as detailed in Table 34, irrespective of the columns you have chosen to display on the page. These fields are not populated if the information is not available for the selected software.

7. Click **Back** at the top left of the page to return to the Device Management page.

RELATED DOCUMENTATION

- Viewing Managed Devices | **194**
- Resynchronizing Managed Devices with the Network | **448**
- Understanding How Junos Space Automatically Resynchronizes Managed Devices | **216**
- Systems of Record in Junos Space Overview | **214**
- Device Images and Scripts Overview | **609**

Exporting the Physical Inventory of Devices

You can export the physical inventory of selected or all devices managed by Junos Space Network Management Platform from the Device Management page as a comma-separated values (CSV) file.

NOTE: You can also export the physical inventory of one or multiple devices managed by Junos Space Platform from the View Physical Inventory page. For more information, refer to "Viewing the Physical Inventory" on page 301.

To export the physical inventory of selected or all devices:

1. On the Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page displays the devices managed by Junos Space Network Management Platform.

2. (Optional) To preview the device information before you export the CSV file, select the devices and select **Device Inventory > View Physical Inventory** from the Actions menu.

   The View Physical Inventory page appears.

3. Select the devices whose physical inventory you want to export and select **Device Inventory > Export Physical Inventory** from the Actions menu.

   The Export Inventory dialog box is displayed.

4. (Optional) Click the plus sign (+) to the left of a device on the list to view more details about the device.

5. Export the physical inventory of the devices.

   a. You can export the physical inventory details of selected or all devices.

      - To export the physical inventory details of selected devices, click **Export Selected**.
      - To export the physical inventory details of all devices, click **Export All**.
      - To cancel the export operation, click **Cancel**.

        You are returned to the Device Management page.

      If you selected to export, the Export Inventory Job Status information dialog box is displayed. When the job is completed, the Export Inventory Job Status report indicates that the job is complete.

   b. Click the **Download** link in the Export Inventory Job Status information dialog box to download the CSV file.

      The CSV file you downloaded displays physical inventory of selected devices or all devices. The details include name of the device, chassis, name of the module, name of the sub-module, name of the sub-sub-module, name of the sub-sub-sub-module, model number of the device, model of the

device, part number of the device, revision number of the device, serial number of the device, vendor part number, vendor material number, and the description provided for the device.

6. Close the Export Inventory Job Status information dialog box to return to the Device Management page.

RELATED DOCUMENTATION

- Device Inventory Overview | **299**
- Device Management Overview | **189**
- Device Discovery Profiles Overview | **220**
- Viewing the Physical Inventory | **301**
- Viewing Managed Devices | **194**

CHAPTER 14

Configuring Juniper Networks Devices

IN THIS CHAPTER

- Modifying the Configuration on the Device | **322**
- Reviewing and Deploying the Device Configuration | **327**
- Junos OS Releases Supported in Junos Space Network Management Platform | **334**
- Configuration Guides Overview | **337**
- Saving the Configuration Created using the Configuration Guides | **337**
- Previewing the Configuration Created using the Configuration Guides | **338**
- Deploying the Configuration Created using the Configuration Guides | **339**
- Viewing and Assigning Shared Objects | **340**
- Applying a CLI Configlet to Devices | **342**
- Applying a CLI Configlet to a Physical Inventory Element | **346**
- Applying a CLI Configlet to a Physical Interface | **350**
- Applying a CLI Configlet to a Logical Interface | **354**
- Executing a Script on the Devices | **358**
- Executing a Script on a Physical Inventory Component | **363**
- Executing a Script on a Logical Interface | **365**
- Executing a Script on the Physical Interfaces | **367**

Modifying the Configuration on the Device

You modify the configuration on a device by using the Modify Configuration page. This topic describes the individual operations involved in modifying a device configuration after you have selected your device and the configuration perspective.

> **NOTE:** You can use this workflow to modify the configuration on modeled devices too.

To modify the device configuration:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Right-click the device whose configuration you want to modify and select **Device Configuration > Modify Configuration**.

   The **Modify Configuration** page is displayed.

3. You can use the Schema-based Configuration Editor or Configuration Guides to modify the device configuration.

   To modify the configuration by using the Schema-based Configuration Editor:

   a. Click the **Schema-based Configuration Editor** link to modify the configuration by using the schema-based editor.

   b. Select a configuration option from the hierarchy in the left pane.

      The contents of the right pane change to reflect your selection on the left, and the full name of the configuration option appears on the title bar on the right pane.

      The parameters of a configuration option that are displayed vary depending on the data type of the option. The data type is shown in a tooltip when you mouse over an option in the hierarchy. It is the data type that determines how the parameter is validated. The data type is in turn determined by the DMI schema .

      The options displayed in table rows can be manipulated as follows:

      - Edited by selecting a row and clicking the diagonal pencil icon
      - Added by clicking the plus icon
      - Deleted by selecting a row and clicking the minus icon

The variety in the data presentation affects only how you arrive at the value you want to change, not the value itself.

For more information about the correlation between data types and validation methods, see “Creating a Template Definition” on page 471.

A parameter available for configuration is usually displayed as the **View/Configure** link.

c. Click **View/Configure** until you arrive at the parameter that you want to change.

d. Make your change.

In the hierarchy on the left, the option you have changed is highlighted and the option label is set in bold. This distinguishes it from subsequent options that you simply visit, without making any changes. If you open the hierarchy, you see not only the name of the principal option, but also the name of the particular parameter that you have changed; for example, not only “SNMP,” but also “Description.”

> **NOTE:** Your edits are saved when you click anywhere else on the Edit Device Configuration page (that is, another configuration option or any of the buttons).

e. (Optional) For information about individual parameters, click the little blue information icons on the right of the configuration settings to display explanations.

f. (Optional) To add comments about individual parameters, click the little yellow comment icons next to the configuration settings and enter your comments.

g. (Optional) To activate or deactivate a configuration option, click the **Activate** or **Deactivate** link respectively.

> **NOTE:** You can activate or deactivate a configuration option only if the configuration node exists.

h. (Optional) In the **Comments** field, enter any remarks that you want to display when the consolidated configuration is reviewed. The remarks appear as a title for the configuration.

If you do not enter anything in this field, the label for the configuration is something similar to **Generated config change from: created by super at 2012-09-14 01:33:26.564 (1 Item)**.

To modify the device configuration by using Configuration Guides:

a. Click the **Basic Setup** link.

   The Basic Setup pop-up window is displayed.

b. (Optional) In the **Hostname** field, enter the hostname of the device.

c. (Optional) In the **Domain name** field, enter the domain name of the device.

d. (Optional) In the **Timezone** field, enter the time zone of the device.

e. (Optional) Select the **Allow FTP file transfers** check box if you want to allow FTP file transfers on the device.

f. (Optional) Select the **Allow ssh access** check box if you want to allow accessing the device through SSH.

g. (Optional) Select the **Allow telnet login** check box if you want to allow logging in to the device through Telnet.

h. For NTP Server, click the Add NTP Server icon to add an NTP server to the device.

   The Add pop-up window is displayed.

   Enter the following details in this pop-up window:

   i. In the **Name** field, enter the name of the NTP server.

   ii. (Optional) In the **Key** field, enter a value for the key.

   iii. (Optional) From the **Version** drop-down list, select the appropriate version.

   iv. (Optional) Select the **Prefer** check box.

   v. Click **Create**.

      Click the Edit NTP Server or Delete NTP Server icon to edit NTP server details or delete the NTP server.

i. For User Management, click the Add User icon to add users for the device.

The Add pop-up window is displayed.

Enter the following details in this pop-up window:

i. In the **Name** field, enter the name of the user.

ii. (Optional) Select an appropriate user ID from the **User ID** field.

The minimum value for this field is 100.

iii. (Optional) In the **Full Name** field, enter the full name of the user.

iv. (Optional) In the **Password** field, enter the password for the user.

v. (Optional) In the **Re-enter Password** field, re-enter the password for the user.

vi. From the **Login Class** drop-down list, select the appropriate login class for the user.

The available login classes are super-user, operator, read-only, unauthorized, and wheel.

vii. Click **Create**.

Click the Edit User or Delete User icon to edit user details or delete the user.

j. For DNS Server, click the DNS NTP Server icon to add a DNS server to the device.

The Add pop-up window is displayed.

Enter the following details in this pop-up window:

i. In the **Name** field, enter the name of the DNS server.

ii. Click **Create**.

Click the Edit DNS Server or Delete DNS Server icon to edit the DNS server details or delete the DNS server.

k. For SNMP, enter the following details:

i. In the **Location** field, enter the location for SNMP.

ii. Click the Add SNMP Community icon.

The Add pop-up window is displayed.

For Community, enter the following details:

a. In the **Name** field, enter the name of the SNMP community.

b. (Optional) From the **Authorization** drop-down list, select the appropriate type of authorization.

c. Click **Create**.

Click the Edit SNMP Community or Delete SNMP Community icon to edit the SNMP Community details or delete the SNMP community.

iii. Click the Add Trap Group icon.

The Add pop-up window is displayed.

For Trap Group, enter the following details:

a. In the **Name** field, enter the name of the trap group.

b. (Optional) Select the check box next to the appropriate trap group category.

c. Click **Create**.

l. Click **OK**.

> **NOTE:** If you have installed the Security Director application on your Junos Space Network Management Platform setup and are modifying the configuration on an SRX Series device, you can use the additional Configuration Guides available on the Modify Configuration page. In this case, the Modify Configuration page lists the Configuration Guides to set up routing and security parameters on an SRX Series device. For more information about using the Configuration Guides related to routing and security parameters on an SRX Series device, see the *Junos Space Security Director Application Guide*.

4. You can preview, save, or deploy the device configuration.

- To preview the configuration before deploying it to the device, click **Preview**.
- To save the configuration, click **Save**.
- To deploy the configuration on the device, click **Deploy**.

> **NOTE:** You cannot validate or deploy the configuration on a modeled device (that is, a device in the Modeled state).

RELATED DOCUMENTATION

Device Management Overview | 189
Reviewing and Deploying the Device Configuration | 327

Reviewing and Deploying the Device Configuration

IN THIS SECTION

- Viewing the Configuration Changes on the Device | 328
- Validating the Delta Configuration on the Device | 330
- Viewing the Device-Configuration Validation Report | 330
- Excluding or Including a Group of Configuration Changes | 331
- Deleting a Group of Configuration Changes | 331
- Approving the Configuration Changes | 332
- Rejecting the Configuration Changes | 333
- Deploying the Configuration Changes to a Device | 333

When you finish modifying a device configuration, you can review and deploy the configuration by using the Review/Deploy Configuration page. You can review and deploy configurations created using the Schema-Based Configuration Editor, CLI Configlets, or Configuration Guides. You can review these configurations in a device-centric view, exclude or include, and approve or reject appropriate configuration changes, and deploy them to one or more devices in a single commit operation.

In Junos Space Network Management Platform, different users can create configuration templates for a particular device. A single reviewer can then view all these configurations for one or multiple devices (see "Viewing and Assigning Shared Objects" on page 340) to decide which of them to deploy and in what sequence.

NOTE: It is possible to create a configuration that is not shared, in which case, only its creator can deploy it. For example, configurations scheduled for deployment that were created with the Schema-Based Configuration Editor are not shared and are therefore not visible as a shared object.

> **NOTE:** You cannot validate or deploy a configuration on a modeled device that is in the Modeled state.

You can perform the following tasks on the Review/Deploy Configuration page:

Viewing the Configuration Changes on the Device

You can view the configuration changes that you want to deploy on the device, on the Review/Deploy Configuration page. The configuration displayed on the page includes changes from the Schema-Based Configuration Editor, templates, or CLI Configlets.

To view the configuration changes:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page appears.

2. Right-click the device whose configuration you want to view and select **Device Configuration > Review/Deploy Configuration**.

   The Review/Deploy Configuration page is displayed. The Selected Devices area on the left side of this page displays the device on which you are about to deploy the configuration. The right side of this page displays the modified configuration that you are about to deploy on the device, on the Change Summary tab.

   For more information about the tabs displayed on this page, see Table 36.

   > **NOTE:** You can also select multiple devices and view the configuration changes on these devices on the Change Summary tab.

   Table 35 shows the columns displayed in the Selected Devices area.

   Table 35: Columns in the Selected Devices Area

Column Name	Description
Device ID	ID of the device
Device Name	Name of the device

Table 35: Columns in the Selected Devices Area *(continued)*

Column Name	Description
Managed Status	Current status of the managed device in Junos Space Network Management Platform. For more information about states in the Managed Status column, see "Viewing Managed Devices" on page 194.
Validation	Validation results of the configuration on the device
Status	Status of the modified configuration on the device: approved, rejected, or deployed

The right side of the page displays different tabs that you can select to view configuration deltas from the running configuration. A delta is the differential configuration that you are about to deploy on the device. Table 36 lists the tabs.

Table 36: Tabs to View Configuration Deltas

Tab Name	Description
Change Summary	Pending configuration changes for the device
Delta Config (CLI)	Deltas from the running configuration in CLI format
Delta Config (XML)	Deltas from the running configuration in XML format
Additional Info	More configuration details to add to the audit trail

NOTE: The configuration changes from the Schema-Based Configuration Editor or templates are shown in the CLI format, whereas the changes from a CLI Configlet are shown only in the curly-braces format. The Delta Config (CLI) and Delta Config (XML) tabs are disabled if the delta configuration includes configuration changes from CLI Configlets.

3. Click the appropriate tab for the details you want to view.

Click **Close** to return to the Review/Deploy Configuration page.

Validating the Delta Configuration on the Device

You validate the delta configuration on the device and view the validation results before deploying the configuration changes to the device. The configuration changes created using the Schema-Based Configuration Editor, templates, and CLI Configlets are validated on the device.

To validate the delta configuration on the device:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page appears.

2. Right-click the device whose configuration you want to validate and select **Device Configuration > Review/Deploy Configuration**.

   The Review/Deploy Configuration page is displayed.

3. On the Change Summary tab, click the **Validate on Device** link.

   A job is created. You can click the Job ID to view the job details.

   > **NOTE:** You cannot validate the configuration if you select a device that is in the Modeled state.

Click **Close** to return to the Review/Deploy Configuration page.

Viewing the Device-Configuration Validation Report

After you have validated the configuration on the device, you can view the validation results.

To view the validation results:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page appears.

2. Right-click the device whose configuration validation report you want to view and select **Device Configuration > Review/Deploy Configuration**.

   The Review/Deploy Configuration page is displayed.

3. On the Change Summary tab, click the **Device Validation Report** link.

A dialog box displays the results of the validation.

Click **Close** to return to the Review/Deploy Configuration page.

Excluding or Including a Group of Configuration Changes

You can exclude or include a specific group of configuration changes created using the Schema-Based Configuration Editor, templates, and CLI Configlets. If you exclude a configuration change, the change is not deployed to the device during the deploy operation.

To exclude or include a specific group of configuration changes:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page appears.

2. Right-click the device whose specific group of configuration changes you want to exclude or include and select **Device Configuration > Review/Deploy Configuration**.

   The Review/Deploy Configuration page is displayed.

3. On the Change Summary tab, click **Exclude** to exclude changes from the template or the Schema-Based Configuration Editor.

   Alternatively, on the Change Summary tab, click **Include** to include any template changes to the configuration that you are deploying to the device.

Click **Close** to return to the Review/Deploy Configuration page.

Deleting a Group of Configuration Changes

You can delete a specific group of configuration changes created using the Schema-Based Configuration Editor, templates, and CLI Configlets. If you delete the configuration changes, the changes are not deployed to the device during the deploy operation.

To delete a specific group of configuration changes:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page appears.

2. Right-click the device whose specific group of configuration changes you want to delete and select **Device Configuration > Review/Deploy Configuration**.

The Review/Deploy Configuration page is displayed.

3. On the Change Summary tab, click **Delete** to delete any changes from the Schema-Based Configuration Editor.

Click **Close** to return to the Review/Deploy Configuration page.

Approving the Configuration Changes

You approve the configuration changes after you have successfully validated the configuration changes on the device. Approving the configuration is the last step you perform before you deploy the configuration on the device.

To approve the configuration changes:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page appears.

2. Right-click the device whose configuration changes you want to approve and select **Device Configuration > Review/Deploy Configuration**.

   The Review/Deploy Configuration page is displayed.

3. Click **Approve** to approve the configuration.

4. Click **Yes** on the confirmation dialog box.

> **NOTE:** If you cannot approve the configuration on the Review/Deploy Configuration page, check whether the **Enable approval workflow for configuration deployment** check box on the Administration > Applications > Modify Application Settings > Devices page is not selected. By default, this check box is selected.

Rejecting the Configuration Changes

You can reject the configuration changes you have approved earlier. Rejecting the configuration changes prevents the configuration from being deployed on the device.

To reject the configuration changes:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page appears.

2. Right-click the device whose configuration changes you want to reject and select **Device Configuration > Review/Deploy Configuration**.

   The Review/Deploy Configuration page is displayed.

3. Select an approved configuration change and click **Reject**.

4. Click **Yes** in the confirmation dialog box.

> **NOTE:** You can view the rejected configuration on the Change Summary tab.

Deploying the Configuration Changes to a Device

You can deploy the configuration changes you have approved earlier to a device.

To deploy the configuration changes to a device:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page appears.

2. Right-click the device whose configuration changes you want to deploy and select **Review/Deploy Configuration**.

   The Review/Deploy Configuration page is displayed.

3. Click **Deploy**.

   The Deploy Configuration dialog box is displayed.

> **NOTE:** If you select a device that is in the Modeled state, the Deploy button appears dimmed.

You can deploy the configuration immediately or later.

- To deploy the configuration to the device immediately, select the **Deploy Now** option button.
- To deploy the configuration to the device later, select **Deploy Later** and specify the date and time.

4. Click **OK**.

   A job is triggered. You can view the details of this job on the Job Management page. The job displays the configuration deployed on the device in two areas—from the Schema-Based Configuration Editor and templates, and from CLI Configlets.

> **NOTE:** If you are upgrading to a new version of Junos Space Network Management Platform, you should deploy all consolidated configurations and change requests before the upgrade. The upgrade deletes all consolidated configurations and change requests.

RELATED DOCUMENTATION

Device Management Overview | 189

Viewing and Assigning Shared Objects | 340

Junos OS Releases Supported in Junos Space Network Management Platform

The following Junos OS software releases are supported in different Junos Space applications:

- Junos OS Release 9.3
- Junos OS Release 9.4
- Junos OS Release 9.5
- Junos OS Release 9.6
- Junos OS Release 10.0
- Junos OS Release 10.1

- Junos OS Release 10.2
- Junos OS Release 10.3
- Junos OS Release 10.4
- Junos OS Release 11.1
- Junos OS Release 11.2
- Junos OS Release 11.3
- Junos OS Release 11.4
- Junos OS Release 12.1
- Junos OS Release 12.2
- Junos OS Release 12.3
- Junos OS Release 13.1
- Junos OS Release 13.2
- Junos OS Release 13.3
- Junos OS Release 14.1
- Junos OS Release 14.2
- Junos OS Release 15.1
- Junos OS Release 16.1
- Junos OS Release 16.2
- Junos OS Release 17.1
- Junos OS Release 17.2
- Junos OS Release 17.3
- Junos OS Release 17.4
- Junos OS Release 18.1
- Junos OS Release 18.2
- Junos OS Release 18.3
- Junos OS Release 18.4
- Junos OS Release 19.1
- Junos OS Release 19.2
- Junos OS Release 19.3
- Junos OS Release 19.4
- Junos OS Release 20.1

Release History Table

Release	Description
20.1	Junos OS Release 20.1
19.4	Junos OS Release 19.4
19.3	Junos OS Release 19.3
19.2	Junos OS Release 19.2
19.1	Junos OS Release 19.1
18.4	Junos OS Release 18.4
18.3	Junos OS Release 18.3
18.2	Junos OS Release 18.2
18.1	Junos OS Release 18.1
17.4	Junos OS Release 17.4
17.3	Junos OS Release 17.3
17.1R1	Junos OS Release 16.2
17.1R1	Junos OS Release 17.1
17.1R1	Junos OS Release 17.2

RELATED DOCUMENTATION

Modifying the Configuration on the Device | **322**

Viewing the Active Configuration | **376**

Juniper Networks Devices Supported by Junos Space Network Management Platform | **199**

Configuration Guides Overview

The Device Management Interface (DMI) schema-based Configuration Editor that is shipped with Junos Space Network Management Platform helps you modify the entire configuration of a device. However, to modify only a part of the configuration of the device, use the custom-built user interface of Configuration Guides.

Configuration Guides are deployed as a single application on the Junos Space Network Management Platform. When you install Junos Space Network Management Platform on a device, the Configuration Guides packaged in the application are automatically displayed on the View/Edit Configuration page. All changes to the device configuration you made using the Configuration Guides are collected as a single change request. The configuration changes you make in one Configuration Guide are visible in other Configuration Guides and the Configuration Editor. If you change a parameter using two Configuration Guides, the change made in the last Configuration Guide is accepted. The changes are merged in chronological order. You can preview the combined configuration changes in XML and CLI formats.

When you have finished editing the device configuration using the Configuration Guides, you can finalize the changes by previewing and saving the changes, or by deploying the changes on the device. Clicking the Deploy button takes you to the Review/Deploy Configuration page.

RELATED DOCUMENTATION

- Saving the Configuration Created using the Configuration Guides | 337
- Previewing the Configuration Created using the Configuration Guides | 338
- Deploying the Configuration Created using the Configuration Guides | 339

Saving the Configuration Created using the Configuration Guides

You can access Configuration Guides from the Devices workspace in Junos Space Network Management Platform. You can save the configuration on Junos Space Network Management Platform.

To save the device configuration created using the Configuration Guides:

1. On the Junos Space Network Management Platform user interface, select **Devices** > **Device Management**.
2. Select the device for which you want to use Configuration Guides.
3. Right-click the device and select **Device Configuration** > **Modify Configuration**.

The Modify Configuration page is displayed. This page lists the Configuration Guides deployed with the hot-plugged application. You can also open the generic configuration editor by clicking the Schema-based Configuration Editor link.

4. Use the Configuration Guides to modify the device configuration.

5. Click **Save**.

RELATED DOCUMENTATION

Configuration Guides Overview | 337

Previewing the Configuration Created using the Configuration Guides | 338

Deploying the Configuration Created using the Configuration Guides | 339

Previewing the Configuration Created using the Configuration Guides

You can access Configuration Guides from the Devices workspace in Junos Space Network Management Platform. You can preview the configuration before deploying it to the devices

To preview the device configuration created using the Configuration Guides:

1. On the Network Management Platform user interface, select **Devices** > **Device Management**.

2. Select the device for which you want to use the Configuration Wizard.

3. Right-click the device and select **Device Configuration** > **Modify Configuration**.

   The Modify Configuration page is displayed. This page lists the Configuration Guides deployed with the hot-plugged application. You can also open the generic configuration editor by clicking the Schema-based Configuration Editor link.

4. Use the Configuration Guides to modify the device configuration.

5. Click **Preview**.

   The View Configuration Change page is displayed. You can view the configuration changes either in the CLI or XML formats.

6. Click **Close**.

RELATED DOCUMENTATION

Configuration Guides Overview | 337

Deploying the Configuration Created using the Configuration Guides

You can access Configuration Guides from the Devices workspace in Junos Space Network Management Platform. You can deploy the configuration on the devices.

To deploy the device configuration using the Configuration Guides:

1. On the Junos Space Network Management Platform user interface, select **Devices** > **Device Management**.
2. Select the device for which you want to use Configuration Guides.
3. Right-click the device and select **Device Configuration** > **View/Edit Configuration**.

   The View/Edit Configuration page is displayed. This page lists the Configuration Guides deployed with the hot-plugged application. You can also open the generic configuration editor by clicking the Schema-based Configuration Editor link.
4. Use the Configuration Guides to modify the device configuration.
5. Click **Deploy**.

   The Deploy Options page is displayed.
6. Select the appropriate deployment schedule from the **Date** and **Time** options.
7. Click **Deploy**.

RELATED DOCUMENTATION

Configuration Guides Overview | 337

Saving the Configuration Created using the Configuration Guides | 337

Previewing the Configuration Created using the Configuration Guides | 338

Viewing and Assigning Shared Objects

Shared object is a template. You assign a shared object to assign the configuration in the template to devices.

You can view the configurations created using Junos Space applications and Junos Space Platform workspaces that are applicable for each device. You can assign and queue them up before deploying them to devices. You can also accept or reject the pending configurations, and you can change the sequence in which these changes are committed. Accepting a configuration is assigning it, and rejecting it is unassigning it.

All configurations that have been created for the device are assigned and will be candidates for deployment, unless you unassign them.

Viewing assigned shared objects can only be done on a per-device basis.

You can select only one device at a time. To view assigned shared objects:

1. On the Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Select the device whose assigned objects you want to view, and select **Device Configuration > View/Assign Shared Objects** from the Actions menu

   The View/Assign Shared Objects page is displayed. It lists the running configuration and the pending configurations on the right and displays the workspaces where these configuration originated from on the left.

   The following Table 37 lists the columns available on this page.

   Table 37: View Assigned Shared Objects Table

Column Heading	Content
Name	Name of the template
Assigned Template Version	Version of the template assigned on the device
Deployment Template Version	Version of the template deployed on the device
Modified By	User who last modified the template
Modify Time	Time when the template was last modified
Description	Description of the template

All of the columns in the table have filtering enabled. Each of the configurations listed can be selected and all of the following can be performed:

- Assign Templates
- Unassign Templates
- Move Up / Move Down

3. If you want to assign a template:
   a. On the left side of the page, select the workspace where the configuration was created.

      The table on the right displays the configurations created in the selected workspace.

   b. Select the check box for the configuration you want to assign, and click the [+] sign.

      The template is assigned.

4. To unassign a template:
   a. On the left side of the page, select the workspace where the configuration was created.

      The table on the right displays the configurations created in the selected workspace.

   b. Select the check box for the configuration you want to unassign, and click the [-] sign.

      A Confirm dialog appears, asking you whether you want to unassign the selected object.

   c. Click **Yes** to dismiss the dialog.

      The template disappears from the table.

5. To change the sequence of objects, assigned or otherwise:
   a. Select the check box for the configuration whose position you want to change, and click the up or the down arrow.

      The object moves up or down in the display as required.

   b. (Optional) Continue moving objects the same way until you are satisfied.

6. Click Assign.

RELATED DOCUMENTATION

Modifying the Configuration on the Device | **322**

Assigning a Device Template to Devices | **496**

Deploying a Template to the Devices | **498**

Applying a CLI Configlet to Devices

CLI Configlets are configuration tools provided by Junos OS that enable you to apply a configuration onto a device by reducing configuration complexity. A CLI Configlet is a configuration template that is transformed into a CLI configuration string before being applied to a device. You apply a CLI Configlet to push a configuration to a device.

> **NOTE:** To easily identify the CLI Configlet that you want to apply to the device, apply a filter on the Reference Number column. You cannot validate a CLI Configlet, or apply a CLI Configlet to more than 200 devices if the CLI Configlet requires XPath processing. However you can apply CLI Configlets to more than 200 devices if the CLI Configlets do not require XPath processing. CLI Configlets that do not require XPath processing include CLI Configlets with context /, //, or */device* and without device-specific or entity-specific parameters.

To apply a CLI Configlet to a device:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Select a device and select **Device Operations** > **Apply CLI Configlet** from the Actions menu.

   The Apply CLI Configlet page is displayed. This page displays the list of CLI Configlets categorized by context and device family.

3. (Optional) To view the context:

   a. Click the **View Context** link.

      The **Context** dialog box is displayed.

   b. Click **OK**.

4. You can filter the list of CLI Configlets that you want to apply to the device manually or by using tags.

   - To filter the CLI Configlets manually, enter the search criteria in the Search field and click the Search icon.

     The list of CLI Configlets is further filtered by the search criteria.

   - To filter the CLI Configlets by using tags:

     a. Click the **Select by tags** option button.

        The Search field disappears.

     b. From the **Select by tags** drop-down list, select an appropriate tag.

c. Click **OK**.

The list of CLI Configlets is further filtered by the tag you selected.

> **NOTE:** This filtered view is retained even when you navigate to other inventory landing pages.

5. Select a CLI Configlet from the filtered list.

   The parameters of the CLI Configlet are displayed.

   From Junos Space Platform Release 17.2R1 onward, you can use CSV files to input parameter values when you need to apply configlets on multiple devices. You can upload the parameter values in the specified format as a CSV file.

   To download a sample CSV file, click the **Download Configlet Parameters** link. The **SampleParameterCSV** file is downloaded with the parameters already present in the editable grid. You can enter or edit the required parameter values in the CSV file easily in addition to manually editing the parameter value field in the grid.

   To upload the edited CSV file, click the **Browse** button, select the file, and then click the **Upload** button. The values of parameters in the CSV file are populated to the editable grid. The parameters of CLI Configlet are listed in the grid with pagination support.

6. (Optional) To enter the values for the parameters of the CLI Configlet, click the appropriate cell in the Value column.
   - If you enter a value for a parameter that is a Password field, the value is hidden.
   - If you enter a value for a parameter that is a Confirm Password field, a pop-up window is displayed. Enter the password again and click **OK**.
7. (Optional) If you want to apply the CLI Configlet later:
   a. Select the **Schedule at a later time** check box.
   b. Enter the date in the **Date** field in the /YYYY format
   c. Enter the time in the **Time** field in the hh:mm format.
8. Click **Next**.

   You can preview the configuration in the CLI Configlet in the Preview area.

The top of the Preview area displays the parameters with the values that are applied to devices. The bottom left of the Preview area displays the devices you have selected. The bottom right of the Preview area displays the configuration that will be applied to the device selected on the left.

- Click a device to view the configuration that will be applied to the device.

9. Before applying the CLI Configlet, you can validate the configuration in the CLI Configlet on the device.

   a. (Optional) To validate the CLI Configlet on the device, click **Validate**.

      The Validate Results page is displayed.

      A job is triggered. The Progress column displays the progress of validation against each device. When the validation is complete, the results of the validation are displayed. The Status column indicates the results of the validation. If the validation is unsuccessful, the details of the error are displayed on the page. If there is an error, the View Job Details page displays an error message. For more information about the error messages, see "Common Error Messages in Device-Related Operations" on page 992.

      > **NOTE:** You can also view the validation results from the Job Management page. To view the validation results, double-click the job ID and click the **View Results** link corresponding to the device. The Validate CLI Configlet Job Remarks pop-up window is displayed. Navigate back to the Validate Results page.

   b. Click **Close** to return to the Apply CLI Configlet page.

10. (Optional) To select a different CLI Configlet or reschedule the workflow, click **Back**.

    You are redirected to the previous page.

11. You can apply the CLI Configlet to the device or submit the configuration changes included in the CLI Configlet to the change requests.

    - To apply the CLI Configlet to the device, click **Apply**.
      - If you selected to apply the CLI Configlet now, the Configlets Results page is displayed.

        A job is triggered. The Progress column displays the progress of applying the CLI Configlet against each device. When the job is complete, the results of the job are displayed. The Status column indicates the results of the job.

> **NOTE:** You can also view the results from the Job Management page. To view the results, double-click the job ID and click the **View Results** link corresponding to the device. The Apply CLI Configlet Job Remarks pop-up window is displayed. Navigate back to the Configlet Results page.

- If you scheduled this task for a later time, the Job Information dialog box displays the schedule information. Click **OK**.

- To submit the configuration changes to the change requests, click **Submit**.

  The configuration changes are included in the list of changes on the Review/Deploy Configuration page in the Devices workspace.

An audit log is generated when you apply or submit the CLI Configlet.

- To cancel this task, click **Cancel**. You are returned to the Device Management page.

Release History Table

Release	Description
17.2	From Junos Space Platform Release 17.2R1 onward, you can use CSV files to input parameter values when you need to apply configlets on multiple devices.

RELATED DOCUMENTATION

CLI Configlets Workflow | 537

CLI Configlets Overview | 534

Creating a CLI Configlet | 548

Applying a CLI Configlet to a Physical Inventory Element

CLI Configlets are configuration tools provided by Junos OS that enables the user to apply a configuration onto a device by reducing configuration complexity. A CLI Configlet is a configuration template that is transformed into a CLI configuration string before being applied to a device. You apply a CLI Configlet to the physical inventory element of a device to push the configuration from the CLI Configlet to the device.

To apply a CLI Configlet to the physical inventory element:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Select a device and select **Device Inventory > View Physical Inventory**.

   The View Physical Inventory page is displayed.

3. Right-click a physical inventory element for which the CLI Configlet has to be applied and select **Apply CLI Configlet**.

   The Apply CLI Configlet page is displayed. This page displays a list of CLI Configlets categorized by context and device family.

4. (Optional) To view the context:

   a. Click the **View Context** link.

      The **Context** dialog box is displayed.

   b. Click **OK**.

5. You can filter the list of CLI Configlets that you want to apply to the physical inventory element manually or by using tags.

   - To filter the CLI Configlets manually, enter the search criteria in the Search field and click the Search icon.

     The list of CLI Configlets is further filtered by the search criteria.

   - To filter the CLI Configlets by using tags:

     a. Click the **Select by tags** option button.

        The Search field disappears.

     b. From the **Select by tags** drop-down list, select an appropriate tag.

     c. Click **OK**.

        The list of CLI Configlets is further filtered by the tag you selected.

> **NOTE:** This filtered view is retained even when you navigate to other inventory landing pages.

6. Select a CLI Configlet from the filtered list.

   The parameters of the CLI Configlet are displayed.

   From Junos Space Platform Release 17.2R1 onward, you can use CSV files to input parameter values when you need to apply configlets on multiple devices. You can upload the parameter values in the specified format as a CSV file.

   To download a sample CSV file, click the **Download Configlet Parameters** link. The **SampleParameterCSV** file is downloaded with the parameters already present in the editable grid. You can enter or edit the required parameter values in the CSV file easily in addition to manually editing the parameter value field in the grid.

   To upload the edited CSV file, click the **Browse** button, select the file, and then click the **Upload** button. The values of parameters in the CSV file are populated to the editable grid. The parameters of CLI Configlet are listed in the grid with pagination support.

7. (Optional) To enter the values for the parameters of the CLI Configlet, click the appropriate cell in the Value column.
   - If you enter a value for a parameter that is a Password field, the value you enter is hidden.
   - If you enter a value for a parameter that is a Confirm Password field, a pop-up window is displayed. Enter the password again and click **OK**.
8. (Optional) If you want to apply the CLI Configlet later:
   a. Select the **Schedule at a later time** check box.
   b. Enter the date in the **Date** field in the MM/DD/YYYY or MM/DD/YY format.
   c. Enter the time in the **Time** field in the hh:mm format.
9. Click **Next**.

   You can preview the configuration in the CLI Configlet in the Preview area.

   The top of the Preview area displays the parameters with the values that are applied to devices. The bottom left of the Preview area displays the devices you have selected. The bottom right of the Preview area displays the configuration that will be applied to the device selected on the left.

10. Before applying the CLI Configlet the physical inventory element of the device, you can validate the configuration in the CLI Configlet on the device.

    a. (Optional) To validate the CLI Configlet on the physical inventory element, click **Validate**.

       The Validate Results page is displayed.

       A job is triggered. The Progress column displays the progress of validation. When the validation is complete, the results of the validation are displayed. The Status column indicates the results of the validation. If the validation is unsuccessful, the details of the error are displayed on the page.

       > **NOTE:** You can also view the validation results from the Job Management page. To view the validation results, double-click the job ID and click the **View Results** link corresponding to the device. The Validate CLI Configlet Job Remarks pop-up window is displayed. Navigate back to the Validate Results page.

    b. Click **Close** to return to the Apply CLI Configlet page.

11. (Optional) To select a different CLI Configlet or reschedule the workflow, click **Back**.

    You are redirected to the previous page.

12. You can apply the CLI Configlet to the physical inventory element or submit the configuration changes included in the CLI Configlet to the change requests.

    - To apply the CLI Configlet to the physical inventory element of the device, click **Apply**.
      - If you selected to apply the CLI Configlet now, the Configlets Results page is displayed.

        A job is triggered. The Progress column displays the progress of applying the CLI Configlet. When the job is complete, the results of the job are displayed. The Status column indicates the results of the job.

        > **NOTE:** You can also view the results from the Job Management page. To view the results, double-click the job ID and click the **View Results** link. The Apply CLI Configlet Job Remarks pop-up window is displayed. Navigate back to the Configlet Results page.

      - If you scheduled to apply this task for later, the Job Information dialog box that appears displays the schedule information. Click **OK**.

- To submit the configuration changes to the change requests, click **Submit**.

  The configuration changes are included in the list of changes on the Review/Deploy Configuration page in the Devices workspace.

An audit log is generated when you apply or submit the CLI Configlet.

- Click **Cancel** to return to the View Physical Inventory page.

Release History Table

Release	Description
17.2	From Junos Space Platform Release 17.2R1 onward, you can use CSV files to input parameter values when you need to apply configlets on multiple devices.

RELATED DOCUMENTATION

- CLI Configlets Workflow | 537
- CLI Configlets Overview | 534
- Applying a CLI Configlet to a Physical Interface | 350
- Applying a CLI Configlet to a Logical Interface | 354

Applying a CLI Configlet to a Physical Interface

CLI Configlets are configuration tools provided by Junos OS that you can use to apply a configuration onto a device more easily. A CLI Configlet is a configuration template that is transformed into a CLI configuration string before being applied to a device. You apply a CLI Configlet to a physical interface of a device to push the configuration from the CLI Configlet to the device.

> **NOTE:** You cannot validate a CLI Configlet or apply a CLI Configlet to more than 200 devices if the CLI Configlet requires XPath processing. However, you can apply CLI Configlets to more than 200 devices if the CLI Configlets do not require XPath processing. CLI Configlets that do not require XPath processing include CLI Configlets with context // and without device- specific or entity-specific parameters.

To apply a CLI Configlet to a physical interface:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Select a device and select **Device Inventory > View Physical Interfaces** from the Actions menu.

   The View Physical Interfaces page is displayed.

3. Right-click a physical interface for which the CLI Configlet has to be applied and select **Apply CLI Configlet**.

   The Apply CLI Configlet page is displayed. This page displays a list of CLI Configlets categorized by context and device family.

4. (Optional) To view the context:

   a. Click the **View Context** link.

      The **Context** dialog box is displayed.

   b. Click **OK**.

5. You can filter the list of CLI Configlets that you want to apply to the physical interface manually or by using tags.

   - To filter the CLI Configlets manually, enter the search criteria in the Search field and click the Search icon.

     The list of CLI Configlets is further filtered by the search criteria.

- To filter the CLI Configlets by using tags:

  a. Click the **Select by tags** option button.

     The Search field disappears.

  b. From the **Select by tags** drop-down list, select an appropriate tag.

  c. Click **OK**.

     The list of CLI Configlets is further filtered by the tag you selected.

     NOTE: This filtered view is retained even when you navigate to other inventory landing pages.

6. Select a CLI Configlet from the filtered list.

   The parameters of the CLI Configlet are displayed.

   From Junos Space Platform Release 17.2R1 onward, you can use CSV files to input parameter values when you need to apply configlets on multiple devices. You can upload the parameter values in the specified format as a CSV file.

   To download a sample CSV file, click the **Download Configlet Parameters** link. The **SampleParameterCSV** file is downloaded with the parameters already present in the editable grid. You can enter or edit the required parameter values in the CSV file easily in addition to manually editing the parameter value field in the grid.

   To upload the edited CSV file, click the **Browse** button, select the file, and then click the **Upload** button. The values of parameters in the CSV file are populated to the editable grid. The parameters of CLI Configlet are listed in the grid with pagination support.

7. (Optional) To enter the value for the parameters of the CLI Configlet, click the appropriate cell in the Value column.

   - If you enter a value for a parameter that is a Password field, the value you enter is hidden.
   - If you enter a value for a parameter that is a Confirm Password field, a pop-up window is displayed. Enter the password again and click **OK**.

8. (Optional) If you want to apply the CLI Configlet later:

   a. Select the **Schedule at a later time** check box.

   b. Enter the date in the **Date** field in the MM/DD/YYYY or MM/DD/YY format.

   c. Enter the time in the **Time** field in the hh:mm format.

9. Click **Next**.

   You can preview the configuration in the CLI Configlet in the Preview area.

The top of the Preview area displays the parameters with the values that are applied to devices. The bottom left of the Preview area displays the devices you have selected. The bottom right of the Preview area displays the configuration that will be applied to the device selected on the left.

10. (Optional) Before you apply the CLI Configlet to a physical interface of a device, validate the configuration in the CLI Configlet on the device.

    a. To validate a CLI Configlet on a physical interface, click **Validate**.

    The Validate Results page is displayed.

    A job is triggered. The Progress column displays the progress of validation. When the validation is complete, the results of the validation are displayed. The Status column indicates the results of the validation. If the validation is unsuccessful, the details of the error are displayed on the page.

    > **NOTE:** You can also view the validation results from the Job Management page. To view the validation results, double-click the job ID and click the **View Results** link. The Validate CLI Configlet Job Remarks pop-up window is displayed. Navigate back to the Validate Results page.

11. (Optional) To select a different CLI Configlet or reschedule the workflow, click **Back**.

    You are redirected to the previous page.

12. You can apply the CLI Configlet to the physical interface or submit the configuration changes included in the CLI Configlet to the change requests.

    - To apply the CLI Configlet to the physical interface of the device, click **Apply**.
      - If you selected to apply the CLI Configlet now, the Configlets Results page is displayed.

        A job is triggered. The Progress column displays the progress of applying the CLI Configlet. When the job is complete, the results of the job are displayed. The Status column indicates the results of the job.

        > **NOTE:** You can also view the results from the Job Management page. To view the results, double-click the job ID and click the **View Results** link. The Apply CLI Configlet Job Remarks pop-up window is displayed. Navigate back to the Configlet Results page.

      - If you scheduled this task for later, the Job Information dialog box that appears displays the schedule information. Click **OK**.

- To submit the configuration changes to the change requests, click **Submit**.
  - The configuration changes are included in the list of changes on the Review/Deploy Configuration page in the Devices workspace.

  An audit log is generated when you apply or submit the CLI Configlet.

- To cancel this task, click **Cancel**. You are returned to the View Physical Interfaces page.

Release History Table

Release	Description
17.2	From Junos Space Platform Release 17.2R1 onward, you can use CSV files to input parameter values when you need to apply configlets on multiple devices.

RELATED DOCUMENTATION

CLI Configlets Workflow | 537

CLI Configlets Overview | 534

Applying a CLI Configlet to a Logical Interface | 354

Applying a CLI Configlet to a Logical Interface

CLI Configlets are configuration tools provided by Junos OS to help you configure a device more easily. A CLI Configlet is a configuration template that is transformed into a CLI configuration string before being applied to a device. You apply a CLI Configlet to the logical interface of a device to push the configuration in the CLI Configlet to the device.

> **NOTE:** You cannot validate a CLI Configlet or apply a CLI Configlet to more than 200 devices if the CLI Configlet requires XPath processing. However, you can apply CLI Configlets to more than 200 devices if the CLI Configlets do not require XPath processing. CLI Configlets that do not require XPath processing include CLI Configlets with context // and without device-specific or entity-specific parameters.

To apply a CLI Configlet to logical interfaces:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Select the required devices and select **Device Inventory > View Logical Interfaces** from the Actions menu.

   The View Logical Interfaces page is displayed with logical interfaces of all the selected devices.

3. Right-click the logical interfaces for which the CLI Configlet must be applied and select **Apply CLI Configlet**.

   The Apply CLI Configlet page is displayed. This page displays a list of CLI Configlets that are categorized by context and device family.

4. (Optional) To view the context:

   a. Click the **View Context** link.

      The **Context** dialog box is displayed.

   b. Click **OK**.

5. You can filter the list of CLI Configlets that you want to apply to the logical interface manually or by using tags.

   - To filter CLI Configlets manually, enter the search criteria in the Search field and click the Search icon.

     The list of CLI Configlets is further filtered by the search criteria.

- To filter the CLI Configlets by using tags:

  a. Click the **Select by tags** option button.

     The Search field disappears.

  b. From the **Select by tags** drop-down list, select an appropriate tag.

  c. Click **OK**.

     The list of CLI Configlets is further filtered by the tag you selected.

     NOTE: This filtered view is retained even when you navigate to other inventory landing pages.

6. Select a CLI Configlet from the filtered list.

   The parameters of the CLI Configlet are displayed.

   From Junos Space Platform Release 17.2R1 onward, you can use CSV files to input parameter values when you need to apply configlets on multiple devices. You can upload the parameter values in the specified format as a CSV file.

   To download a sample CSV file, click the **Download Configlet Parameters** link. The **SampleParameterCSV** file is downloaded with the parameters already present in the editable grid. You can enter or edit the required parameter values in the CSV file easily in addition to manually editing the parameter value field in the grid.

   To upload the edited CSV file, click the **Browse** button, select the file, and then click the **Upload** button. The values of parameters in the CSV file are populated to the editable grid. The parameters of CLI Configlet are listed in the grid with pagination support.

7. (Optional) To enter the values for the parameters of the CLI Configlet, click the appropriate cell in the Value column.

   - If you enter a value for a parameter that is a Password field, the value you enter is hidden.
   - If you enter a value for a parameter that is a Confirm Password field, a pop-up window is displayed. Enter the password again and click **OK**.

8. (Optional) If you want to apply the CLI Configlet later:

   a. Select the **Schedule at a later time** check box.

   b. Enter the date in the **Date** field in the MM/DD/YYYY or MM/DD/YY format.

   c. Enter the time in the **Time** field in the hh:mm format.

9. Click **Next**.

   You can preview the configuration in the CLI Configlet in the Preview area.

The top of the Preview area displays the parameters with the values that are applied to devices. The bottom left of the Preview area displays the devices you have selected. The bottom right of the Preview area displays the configuration that will be applied to the device selected on the left.

10. Before applying the CLI Configlet to the logical interface of the device, you can validate the configuration in the CLI Configlet on the device.

    a. (Optional) To validate the CLI Configlet on the logical interface, click **Validate**.

       The Validate Results page is displayed.

       A job is triggered. The Progress column displays the progress of validation. When the validation is complete, the results of the validation are displayed. The Status column indicates the results of the validation. If the validation is unsuccessful, the details of the error are displayed on the page.

       > **NOTE:** You can also view the validation results from the Job Management page. To view the validation results, double-click the job ID and click the **View Results** link. The Validate CLI Configlet Job Remarks pop-up window is displayed. Navigate back to the Validate Results page.

    b. Click **Close** to return to the Apply CLI Configlet page.

11. (Optional) To select a different CLI Configlet or reschedule the workflow, click **Back**.

    You are redirected to the previous page.

12. You can apply the CLI Configlet to the logical interface of multiple devices or submit the configuration changes included in the CLI Configlet to the change requests.

    - To apply the CLI Configlet to the logical interface of devices, click **Apply**.
      - If you selected to apply the CLI Configlet, the Configlets Results page is displayed.

        A job is triggered. The Progress column displays the progress of applying the CLI Configlet. When the job is complete, the results of the job are displayed. The Status column indicates the result of the job.

        > **NOTE:** You can also view the results from the Job Management page. To view the results, double-click the job ID and click the **View Results** link. The Apply CLI Configlet Job Remarks pop-up window is displayed. Navigate back to the Configlet Results page.

- If you scheduled the apply the CLI Configlet task for later, the Job Information dialog box displays the schedule information. Click **OK**.

- To submit the configuration changes to the change requests, click **Submit**.

  The configuration changes are included in the list of changes on the Review/Deploy Configuration page in the Devices workspace.

  An audit log is generated when you apply or submit the CLI Configlet.

13. To cancel the task, click **Cancel**. You are returned to the View Logical Interfaces page.

Release History Table

Release	Description
17.2	From Junos Space Platform Release 17.2R1 onward, you can use CSV files to input parameter values when you need to apply configlets on multiple devices.

RELATED DOCUMENTATION

CLI Configlets Workflow | 537

CLI Configlets Overview | 534

Applying a CLI Configlet to a Physical Interface | 350

Executing a Script on the Devices

You can execute op scripts on one or more devices simultaneously by using the Devices workspace in Junos Space Network Management Platform. Commit and event scripts are automatically activated after they are enabled. Commit scripts are triggered every time a commit is called on the device and event scripts are triggered every time an event occurs on the device or if a time is specified.

> **NOTE:** You can execute scrips on more than 200 devices only if the scripts do not require XPath processing. Scripts that do not require XPath processing include scripts without device-specific or entity-specific parameters and with /, //, or /device as context.

To execute a script on selected devices by using the Devices workspace:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Right-click the devices and select **Device Operations** > **Execute Scripts**.

   The Execute Scripts page displays the following scripts:

   - Scripts that are associated with and enabled (device scripts) on the selected devices
   - Scripts whose execution type matches your selection. If you selected multiple devices, only scripts whose EXECUTIONTYPE is set to GROUPEDEXECUTION are displayed. If you selected a single device, scripts whose EXECUTIONTYPE is set to SINGLEEXECUTION and GROUPEDEXECUTION are displayed.
   - Scripts whose context matches the device context

   Table 38 lists the columns on the Execute Scripts page and their descriptions.

   Table 38: Execute Scripts Page in the Devices Workspace

Column	Description
Script Name	Name of the script file
Descriptive Name	Descriptive name of the script
Category	Category of the script
Description	Description of the script
Created Time	Date and time when the script was created

Table 38: Execute Scripts Page in the Devices Workspace *(continued)*

Column	Description
Last Updated Time	Date and time when the script was last updated

3. (Optional) To view the context:
   a. Click the **View Context** link.

      The **Context** dialog box is displayed.

   b. Click **OK** to close the dialog box.

4. Select the script that you want to execute on the devices manually or by using tags.
   - To select the script manually:
     i. Click the **Select Manually** option button.
        This option button is selected by default.
     ii. Select the script.
   - To select the script by using tags:
     i. Click the **Select by tags** option button.
     ii. From the **Select by tags** drop-down list, select an appropriate tag.
     iii. Click **OK**.
        The list of scripts is further filtered by the tag you selected.
     iv. Select the script.
5. (Optional) Click the **Value** column and enter the values for the parameters of the selected script.
6. Select whether to execute the script now or schedule the execution for a later time:
   - To execute the script on the devices now:
     i. Click **Execute**.
        The Script Results page appears. Table 39 lists the columns and their descriptions.

        Table 39: Script Results Page

Column	Description
Job Id	Job ID of the job triggered for executing the script
Script Name	Name of the script
Device Name	

Table 39: Script Results Page *(continued)*

Column	Description
	Name of the device as stored in the Junos Space Platform database If you are executing a device script that contains the EXECUTIONTYPE set to GROUPEDEXECUTION on multiple devices or physical interfaces of multiple devices, the Script Results page displays multiple rows listing the devices in this column. If you are executing a local script that contains the GROUPBYDEVICE annotation set to TRUE on multiple devices or physical interfaces of multiple devices, the Script Results page displays multiple rows listing the devices in this column. If you are executing a local script that does not contain the GROUPBYDEVICE annotation or the GROUPBYDEVICE annotation is set to FALSE on multiple devices or physical interfaces of multiple devices, this column displays the Devices hyperlink. Click the hyperlink to view the list of devices on which the script is executed.
Node IP	IP address of the Junos Space node to which the device is connected
Node Name	Name of the Junos Space node to which the device is connected
Progress	Progress of the job
Status	Completion status of the job: SUCCESS or FAILED

The lower area of the Script Results page displays the results of the script execution. If you executed a local script that contains the GROUPBYDEVICE annotation set to TRUE on multiple devices, click the appropriate device in the Device Name column to view the results of the script execution on the device.

ii. (Optional) To view the list of devices on which the script was executed:

   i. Click the **Devices** hyperlink in the Device Name column.

      The Device Name List information dialog box is displayed with the list of devices.

   ii. Click **Ok** to close the information dialog box.

iii. Click **Close** (at the bottom of the page).

   You are redirected to the Device Management page.

- To schedule the execution of the script on the devices for a later time:

   i. Select the **Schedule at a later time** check box.

ii. Enter the date in the **Date** field in the MM/DD/YYYY format.

iii. Enter the time in the **Time** field in the hh:mm format.

iv. Click **Execute**.

The Job Information dialog box displays a link to the job ID. Click the *Job ID* link to view the status of this task on the Job Management page.

v. Click **OK** to close the Job Information dialog box.

You are redirected to the Device Management page.

RELATED DOCUMENTATION

- Device Inventory Overview | **299**
- Device Images and Scripts Overview | **609**
- Viewing Script Execution | **437**
- Viewing Associated Scripts | **437**

Executing a Script on a Physical Inventory Component

You can use Junos Space Network Management Platform to trigger the execution of op scripts on one or more devices simultaneously. Commit and event scripts are automatically activated after they are enabled. Commit scripts are triggered every time a commit is called on the device and event scripts are triggered every time an event occurs on the device or if a time is specified.

> **NOTE:** You can execute scrips on more than 200 devices only if the scripts do not require XPath processing. Scripts that do not require XPath processing include scripts without device-specific or entity-specific parameters and with /, //, or /device as context.

To execute a script on the physical inventory component of a device:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Select the device and select **Device Inventory** > **View Physical Inventory** from the Actions menu.

3. Right-click a physical inventory element for which the script has to be applied and select **Execute Scripts**.

   The Execute Scripts page is displayed. This page displays the list of scripts that match the context and are enabled and associated with the devices.

4. Select a script from the list.

   - You can also filter the list by using tags and then select a script. To filter the list by using tags:

     a. Click the **Select by tags** option button.

     b. From the **Select by tags** drop-down list, select an appropriate tag.

     c. Click **OK**.

        The list of scripts is filtered by the tag you selected.

     d. Select a script from the filtered list.

5. (Optional) To enter the values for the parameters of the script, click the appropriate cell in the Value column.

   - If you enter a value for a parameter that is a Password field, the value is hidden.
   - If you enter a value for a parameter that is a Confirm Password field, a dialog box is displayed. Enter the password again and click **OK**.

6. You can execute the script now or schedule this task for later:

   To execute the script later:

   a. Select the **Schedule at a later time** check box.

   b. Enter the date in the **Date** field in the DD/MM/YYYY format.

   c. Enter the time in the **Time** field in the hh:mm format.

   To execute the script now:

   - Click **Execute**.

7. If you selected to apply the script now, the Script Results page is displayed. This page shows the progress and status of the job.

   > **NOTE:** If you wait for the job to complete, you can view the job results. Click **Close**.

   If you scheduled this task for later, the Job Information dialog box that appears displays the schedule information. Click **OK**.

Click **Cancel** to return to the Device Management page.

RELATED DOCUMENTATION

Applying a CLI Configlet to a Physical Inventory Element | 346

Executing a Script on a Logical Interface

You can use Junos Space Network Management Platform to trigger the execution of op scripts on one or more devices simultaneously. Commit and event scripts are automatically activated after they are enabled. Commit scripts are triggered every time a commit is called on the device and event scripts are triggered every time an event occurs on the device or if a time is specified.

> **NOTE:** You can execute scrips on more than 200 devices only if the scripts do not require XPath processing. Scripts that do not require XPath processing include scripts without device-specific or entity-specific parameters and with /, //, or /device as context.

To execute a script on the logical interface of devices:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Select the devices and select **Device Inventory** > **View Logical Interfaces** from the Actions menu.

   The View Logical Interfaces page is displayed.

3. Right-click the logical interfaces for which the script has to be applied and select **Execute Scripts**.

   The Execute Scripts page is displayed. This page displays a list of scripts that match the context and are enabled and associated with the devices.

4. Select the script from the list.

   - You can also filter the list by using tags and then select a script. To filter the list by using tags:

     a. Click the **Select by tags** option button.

     b. From the **Select by tags** drop-down list, select an appropriate tag.

     c. Click **OK**.

        The list of scripts is filtered by the tag you selected.

     d. Select a script from the filtered list.

5. (Optional) To enter the values for the parameters of the script, click the appropriate cell in the Value column.

   - If you enter a value for a parameter that is a Password field, the value you enter is hidden.

- If you enter a value for a parameter that is a Confirm Password field, a pop-up window is displayed. Enter the password again and click **OK**.

6. You can execute the script now or schedule this task for later:

   To execute the script later:

   a. Select the **Schedule at a later time** check box.

   b. Enter the date in the **Date** field in the DD/MM/YYYY format.

   c. Enter the time in the **Time** field in the hh:mm format.

   To execute the script now:

   - Click **Execute**.

7. If you selected to apply the script now, the Script Results page is displayed. This page shows the progress and status of the job.

   > **NOTE:** If you wait for the job to complete, you can view the job results. Click **Close**.

   If you scheduled this task for later, the Job Information dialog box displays the schedule information. Click **OK**.

8. Click **Cancel** to return to the Device Management page.

RELATED DOCUMENTATION

Executing a Script on the Devices | 358

Executing a Script on the Physical Interfaces | 367

Executing a Script on the Physical Interfaces

You can use Junos Space Network Management Platform to trigger the execution of op scripts on one or more devices simultaneously. Commit and event scripts are automatically activated after they are enabled. Commit scripts are triggered every time a commit is called on the device and event scripts are triggered every time an event occurs on the device or if a time is specified.

You can execute a script on the physical interfaces of one device or multiple devices.

> **NOTE:** You can execute scrips on more than 200 devices only if the scripts do not require XPath processing. Scripts that do not require XPath processing include scripts without device-specific or entity-specific parameters and with /, //, or /device as context.

To execute a script on the physical interfaces:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Select the device (or multiple devices) and select **Device Inventory** > **View Physical Interfaces** from the Actions menu.

   The View Physical Interfaces page is displayed.

3. Right-click the physical interfaces on which the script has to be executed and select **Execute Scripts**.

   The Execute Scripts page displays the following scripts:

   - Scripts that are associated with and enabled (device scripts) on the selected devices
   - Scripts whose execution type matches your selection. If you selected multiple devices, only scripts whose EXECUTIONTYPE is set to GROUPEDEXECUTION are displayed. If you selected a single device, scripts whose EXECUTIONTYPE is set to SINGLEEXECUTION and GROUPEDEXECUTION are displayed.
   - Scripts whose context matches the physical interface context

   The Table 38 table lists the columns on the Execute Scripts page and their descriptions.

4. Select the script that you want to execute on the physical interfaces manually or by using tags.
   - To select the script manually:
     i. Click the **Select Manually** option button.

        This option button is selected by default.

     ii. Select the script.
   - To select the script by using tags:
     i. Click the **Select by tags** option button.

     ii. From the **Select by tags** drop-down list, select an appropriate tag.

     iii. Click **OK**.

        The list of scripts is further filtered by the tag you selected.

     iv. Select the script.
5. (Optional) To enter the values for the parameters of the script, click the appropriate cell in the **Value** column.
   - If you enter a value for a parameter that is a Password field, the value you enter is hidden.

- If you enter a value for a parameter that is a Confirm Password field, a pop-up window is displayed. Enter the password again and click **OK**.

6. Select whether to execute the script now or schedule the execution for a later time:

- To execute the script on the physical interfaces now:

  i. Click **Execute**.

     The Script Results page appears. The Table 39 table lists the columns and their descriptions.

     The lower area of the Script Results page displays the results of the script execution. If you executed a local script that contains the GROUPBYDEVICE annotation set to TRUE on the physical interfaces of multiple devices, click the appropriate device in the Device Name column to view the script execution results on the physical interface of the device.

  ii. Click **Close** (at the bottom of the page).

     You are redirected to the View Physical Interfaces page.

  iii. Click **Back** (at the top-left corner) to return to the Device Management page.

- To schedule the execution of the script on the physical interfaces for a later time:

  i. Select the **Schedule at a later time** check box.

  ii. Enter the date in the **Date** field in the MM/DD/YYYY format.

  iii. Enter the time in the **Time** field in the hh:mm format.

  iv. Click **Execute**.

     The Job Information dialog box displays a link to the job ID. Click the *Job ID* link to view the status of this task on the Job Management page.

  v. Click **OK** to close the Job Information dialog box.

     You are redirected to the View Physical Interfaces page.

  vi. Click **Back** (at the top-left corner) to return to the Device Management page.

RELATED DOCUMENTATION

Executing a Script on the Devices | 358

CHAPTER 15

Device Adapter

IN THIS CHAPTER

- Worldwide Junos OS Adapter Overview | 371
- Installing the Worldwide Junos OS Adapter | 372
- Connecting to ww Junos OS Devices | 374

Worldwide Junos OS Adapter Overview

The Junos Space wwadapter enables you to manage devices running the worldwide version of Junos OS (ww Junos OS devices) through Junos Space Network Management Platform. ww Junos OS devices use Telnet instead of Secure Shell (SSH2) to communicate with other network elements. Junos Space Network Management Platform uses the failover approach when identifying a ww Junos OS device. It first tries to initiate a connection to the device using SSH2. If it cannot connect to the device, Junos Space Network Management Platform identifies the device as a ww Junos OS device. Since Junos Space Network Management Platform does not support Telnet, it uses an adapter to communicate with ww Junos OS devices. Junos Space Network Management Platform connects to the adapter using SSH2 and the adapter starts a Telnet session with the device.

NOTE: For ww Junos OS devices, Space as a System of Record (SSOR) mode of device management is not supported.

Before you install the wwadapter, complete the following prerequisites:

- Download the adapter image from the local client workstation.
- Ensure that the Junos Space servers have been deployed and are able to access devices.
- Configure Junos Space Network Management Platform to initiate connections with the device.

NOTE: Ensure that you allow at least three Telnet connections between the ww Junos OS device and the Junos Space server. Junos Space Network Management Platform needs a minimum of three Telnet connections with the device in order to be able to manage it.

NOTE: For ww Junos OS devices, the Junos Space Service Now application works only on AI-Scripts version 2.5R1 and later.

The Secure Console workspace and the option in the right-click context menu in the Manage Devices workspace are disabled for ww Junos OS devices.

RELATED DOCUMENTATION

Installing the Worldwide Junos OS Adapter | 372

Connecting to ww Junos OS Devices | 374

Installing the Worldwide Junos OS Adapter

You can install and use the wwadapter to manage devices running on the worldwide version of Junos OS (ww Junos OS devices). Before you install the wwadapter, you must upload the ww Junos OS device wwadapter image file.

To upload the wwadapter image file:

1. On the Junos Space Network Management Platform user interface, select **Devices** > **Device Adapter** .

   The Device Adapter page is displayed.

2. Select the Add Device Adapter icon on the Actions bar.

3. Browse to the wwadapter image file and select the filename so that the full path appears in the Software File field.

4. Click **Upload** to bring the image into Junos Space Network Management Platform.

A status box shows the progress of the image upload. Adding the wwadaptor image file automatically installs the wwadapter.

Before you connect to any device, you must verify that the installation was successful.

To verify that the installation was successful, look at the device console on the Junos Space server.

1. On the server, change the directories to verify that the wwadapter directory has been created.

   ```
   cd /home/jmp/wwadapter
   ```

2. To verify that the wwadapter is running, enter the following command on the Junos Space server:

   ```
   prompt > service wwadapter status
   wwadapter running
   ```

   If the wwadapter is not active, you see the following status:

   ```
   wwadapter stopped
   ```

   Use the following commands to start or stop the wwadapter:

   To start the wwadapter:

   ```
   service wwadapter start
   ```

   To stop the wwadapter:

   ```
   prompt > ps –ef | grep wwadapter
     promt > kill -9 {wwadapter pid}
   ```

To see the wwAdapter logs, change the directories to the wwadapter directory.

```
cd /home/jmp/wwadapter/var/errorLog/DmiAdapter.log
```

To view the contents of the error log file, open the log file with any standard text editor.

To view the contents of the log4j configuration file, change the directories to the wwadapter directory.

```
cd /home/jmp/wwadapter /wwadapterlog4j.lcf
```

RELATED DOCUMENTATION

Worldwide Junos OS Adapter Overview | 371

Connecting to ww Junos OS Devices | 374

Connecting to ww Junos OS Devices

A device running worldwide Junos OS (ww Junos OS device) cannot initiate a connection with Junos Space Network Management Platform. Junos Space Network Management Platform must initiate the connection to the device. To configure this setting:

1. On the Junos Space Network Management Platform user interface, select **Administration** > **Applications**.

   The Applications page is displayed.

2. Select **Network Management Platform** and select **Modify Application Settings** from the Actions menu.

   The Modify Application Settings page appears.

3. Select **Junos Space initiates connection to device**.

4. Select **Support ww Junos Devices** so that Junos Space Network Management Platform can connect to a ww Junos OS device using the wwadapter.

After Junos Space Network Management Platform has discovered the ww Junos OS device through the wwadapter, it manages the device just as it would manage a device that runs the domestic version of Junos OS. For more information about device discovery, refer to "Device Discovery Profiles Overview" on page 220.

NOTE: The SSH to Device option is disabled for ww Junos OS devices.

NOTE: If you are not able to discover the WW Junos OS device , make sure that the NMAP utility returns 'telnet' as open for port 23 on the device.

```
$ nmap –p23 < Device IP >
```

RELATED DOCUMENTATION

Worldwide Junos OS Adapter Overview | 371

Installing the Worldwide Junos OS Adapter | 372

CHAPTER 16

Device Configuration Management

IN THIS CHAPTER

- Viewing the Active Configuration | 376
- Viewing the Configuration Change Log | 381
- Resolving Out of band Changes | 382
- Creating a Quick Template from the Device Configuration | 384

Viewing the Active Configuration

Before you modify the configuration on a device, you need to view the current active configuration on the device. To view all the configuration options for a device, you need to upload the appropriate DMI schema to Junos Space Network Management Platform. If you have not uploaded the appropriate DMI schema for the device, Junos Space Platform uses the default DMI schema for the device.

To view the active configuration on the device:

1. On the Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Right-click the device whose active configuration you want to view and select **Device Configuration > View Active Configuration**.

   The **View Active Configuration** page is displayed.

   You can view the Junos OS statement hierarchy in the left pane. The right pane displays the CLI view of the active configuration on the device, and custom configuration views configured from the CLI Configlets workspace. You can also apply CLI Configlets that match the context of the device.

   By default, the right pane displays the Default View tab (active configuration on the device).

3. (Optional) To view multiple configuration options simultaneously in the right pane:

   a. Click the Custom Settings icon in the left pane.

      The Modify Custom Settings page is displayed.

b. Select the **Enable Multiselect** check box.

c. Click **OK**.

Multiple configuration options are displayed in the right pane.

4. (Optional) To view the configuration options in alphabetical order:

a. Select the Custom Settings icon in the left pane.

The Modify Custom Settings page is displayed.

b. Select the **Enable Alphabetic Ordering** check box.

c. Click **OK**.

The configuration options are displayed in alphabetical order in the left pane and the right pane.

NOTE: The Enable Alphabetical Ordering feature is enabled only for your user account.

5. (Optional) To add a configuration filter and view a specific set of configuration options, click the Create Filter icon in the left pane.

The Add Configuration Filter page is displayed.

For more information, see "Creating a Configuration Filter" on page 605.

6. (Optional) Click the Edit filter icon to modify an existing configuration filter.

7. (Optional) Click the Delete filter icon to delete the existing configuration filters.

8. (Optional) To view the configuration on the device by the custom configuration view created from the CLI Configlets workspace, click the tab for that configuration view.

For example, a configuration view Example 1 assigned to the Global domain displays a tab named Global/Example1.

The right pane displays the configuration of the device as specified by format in the configuration view.

9. (Optional) To view the configuration of the device in CLI format, click the **Default View** tab in the right pane.

The right pane displays the current configuration of the device.

10. (Optional) To refresh the CLI view of the device configuration, click the **Refresh** icon in the right pane.

11. (Optional) To apply a CLI Configlet or submit the changes from a CLI Configlet to the change request of the device, click the **Configure** tab in the right pane.

    a. You can filter the list of CLI Configlets that you want to apply to the device manually or by using tags.

    - To filter the CLI Configlets manually, enter the search criteria in the Search field and click the Search icon.

      The list of CLI Configlets is further filtered by the search criteria.

    - To filter the CLI Configlets by using tags:

      a. Click the **Select by tags** option button.

         The Search field disappears.

      b. From the **Select by tags** drop-down list, select an appropriate tag.

      c. Click **OK**.

         The list of CLI Configlets is further filtered by the tag you selected.

         NOTE: This filtered view is retained even when you navigate to other inventory landing pages.

    b. Select a CLI Configlet from the filtered list.

       The parameters of the CLI Configlet are displayed.

       From Junos Space Platform Release 17.2R1 onward, you can use CSV files to input parameter values when you need to apply configlets on multiple devices. You can upload the parameter values in the specified format as a CSV file.

       To download a sample CSV file, click the **Download Configlet Parameters** link. The **SampleParameterCSV** file is downloaded with the parameters already present in the editable grid. You can enter or edit the required parameter values in the CSV file easily in addition to manually editing the parameter value field in the grid.

       To upload the edited CSV file, click the **Browse** button, select the file, and then click the **Upload** button. The values of parameters in the CSV file are populated to the editable grid. The parameters of CLI Configlet are listed in the grid with pagination support.

    c. (Optional) To enter the values for the parameters of the CLI Configlet, click the appropriate cell in the Value column.

    - If you enter a value for a parameter that is a Password field, the value is hidden.

- If you enter a value for a parameter that is a Confirm Password field, a pop-up window is displayed. Enter the password again and click **OK**.

d. (Optional) If you want to apply the CLI Configlet later:

   a. Select the **Schedule at a later time** check box.

   b. Enter the date in the **Date** field in the DD/MM/YYYY format.

   c. Enter the time in the **Time** field in the hh:mm format.

e. Click **Next**.

   You can preview the configuration in the CLI Configlet in the Preview area.

   The top of the Preview area displays the parameters with the values that are applied to devices. The bottom left of the Preview area displays the devices you have selected. The bottom right of the Preview area displays the configuration that will be applied to the device selected on the left.

   - Click a device to view the configuration that will be applied to the device.

f. Before applying the CLI Configlet, you can validate the configuration in the CLI Configlet on the device.

   i. (Optional) To validate the CLI Configlet on the device, click **Validate**.

      The Validate Results page is displayed.

      A job is triggered. The Progress column displays the progress of validation against each device. When the validation is complete, the results of the validation are displayed. The Status column indicates the results of the validation. If the validation is unsuccessful, the details of the error are displayed on the page.

      > **NOTE:** You can also view the validation results from the Job Management page. To view the validation results, double-click the job ID and click the **View Results** link corresponding to the device. The Validate CLI Configlet Job Remarks pop-up window is displayed. Navigate back to the Validate Results page.

   ii. Click **Close** to return to the Apply CLI Configlet page.

g. (Optional) To select a different CLI Configlet or reschedule the workflow, click **Back**.

You are redirected to the previous page.

h. You can apply the CLI Configlet to the device or submit the configuration changes included in the CLI Configlet to the change requests.

- To apply the CLI Configlet to the device, click **Apply**.

  If you selected to apply the CLI Configlet now, the Configlets Results page is displayed.

  A job is triggered. The Progress column displays the progress of applying the CLI Configlet against each device. When the job is complete, the results of the job are displayed. The Status column indicates the results of the job.

  > **NOTE:** You can also view the results from the Job Management page. To view the results, double-click the job ID and click the **View Results** link corresponding to the device. The Apply CLI Configlet Job Remarks pop-up window is displayed. Navigate back to the Configlet Results page.

  - Click **Close**, You are returned to the View Active Configuration page.

  - If you scheduled this task for a later time, the Job Information dialog box that appears displays the schedule information. Click **OK**.

- To submit the configuration changes to the change requests, click **Submit**.

  The configuration changes are included in the list of changes on the Review/Deploy Configuration page in the Devices workspace.

An audit log is generated when you apply or submit the CLI Configlet.

> **NOTE:** You can select the Enable Alphabetical Ordering check box if you want to view the device configuration by using a configuration filter. The configuration options displayed in the filtered view are sorted in alphabetical order.

Click **Back** on the top-left corner of the View Active Configuration page to go back to the Device Management page.

Release History Table

Release	Description
17.2	From Junos Space Platform Release 17.2R1 onward, you can use CSV files to input parameter values when you need to apply configlets on multiple devices.

RELATED DOCUMENTATION

Viewing Managed Devices | 194

Modifying the Configuration on the Device | 322

Viewing the Configuration Change Log

When Junos Space Network Management Platform is the system of record, users may make out-of-band configuration changes to network devices by manually using the device's management CLI, but there is no automatic resynchronization with the Junos Space Network Management Platform database.

By viewing the configuration change log, you can see the history and details of all device configuration changes, whether initiated from Junos Space Network Management Platform or not. You can investigate details of the changes that were made, and you can decide to accept or reject the changes. If you accept them, the Junos Space Network Management Platform database is updated to reflect the new configuration. If you reject them, the device's out-of-band configuration changes are reverted.

Viewing the Configuration Change Log enables you to resolve out of band changes, which are those changes made on the device itself. When the mode in Network Management Platform > Administration > Applications > Modify Application Settings > Device is Space as the System of Record (SSOR), the system tracks both in-band (Space) and out-of-band (non-Space) changes. When the mode in Application Settings is Network as the System of Record (NSOR) (the default), the system tracks only in-band (Space) changes.

To view configuration change log:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.
   The Device Management page is displayed.

2. Select the device whose configuration log you want to see.

3. Select **Device Configuration > View Configuration Change Log** from the Actions menu.
   The configuration change log is displayed. Table 40 describes its contents.

Table 40: Configuration Change Log

Column Name	Description
Timestamp	The date and time at which the configuration change was made.
Author	The user ID of the person who made the change. For an in-band change, this is the Junos Space username; for and out-of-band change, it is the credential used to log into the CLI management interface.
Configuration Changes	A link to a View Configuration Change XML window in which the details of the change for this device are shown as XML.
Change Type	The type of the change: in band or out of band. Out-of-band changes are further denoted as Outstanding, Accepted, or Rejected.
Application Name	The name of the Junos Space application from which the change was requested.
Commit Comments	The commit comments included in the system log entry related to committing this change. These may include notes from the user who made the commit, as well as the timestamp and username.

RELATED DOCUMENTATION

Resolving Out of band Changes | 382

Reviewing and Deploying the Device Configuration | 327

Resolving Out of band Changes

You can resolve the Out-of-band changes and either accept or reject the configuration changes.

To resolve the out of band changes:

1. On the Junos Space Network Management Platform user interface, select **Network Management Platform > Devices > Device Management**.
   The Device Management page is displayed.

2. Select the device whose out-of-band configuration changes you want to resolve.

3. Select **Device Configuration > Resolve Out-of-band Changes** from the Actions menu.

The Resolve Out-of-band Changes page is displayed. Table 41 describes the columns on this page.

Table 41: Resolving Out-of-Band Changes

Column Name	Description
ID	ID of the configuration change entry
changeXML	The list of out-of-band changes in XML format
device ID	ID of the device
Device Name	Name of the device
Timestamp	The date and time at which the configuration change was made
Author	The user ID of the person who made the change. For out-of-band change, this is the credential used to log into the device CLI management interface.
Configuration Change	A link to the out-of-band changes in XML format
Action	Option buttons enabling you to select Accept or Reject

4. (Optional) To view the out-of-band change:
   a. Click the **View** link in the appropriate row.

      The Out-of-band Change XML pop-up window displays the out-of-band changes in XML format.

   b. Click **OK** to close the pop-up window.

5. You can accept or reject individual changes or accept all the out-of-band changes.
   - To approve or reject individual out-of-band changes:
     i. Select **Accept** or **Reject** in the appropriate row.

     ii. Click **Submit**.

         The Job Information dialog box is displayed with the job ID.

     iii. Click **OK**.

          You are redirected to the Device Management page.

- To approve all the out-of-band changes:

  i. Click **Accept All**.

  ii. Click **Submit**.

  The Job Information dialog box is displayed with the job ID.

  iii. Click **OK**.

  You are redirected to the Device Management page.

RELATED DOCUMENTATION

Viewing the Configuration Change Log | 381

Reviewing and Deploying the Device Configuration | 327

Creating a Quick Template from the Device Configuration

You create a quick template from a device configuration when you want to push this configuration to multiple devices by deploying the quick template. You create a quick template from a device configuration from the Devices workspace.

To create a quick template from the device configuration:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management** .

   The Device Management page is displayed.

2. Right-click the device whose configuration you want to migrate to a quick template and select **Device Configuration > Create Template from Device Configuration** from the contextual menu.

   You are redirected to the Create Quick Template page in the Device Templates workspace. You can modify the Name field, and add or modify the device configuration using the CLI-based or Form-based editor.

3. Use the Create Quick Template workflow to create a quick template from the device configuration. For more information, see "Creating a Quick Template" on page 509.

RELATED DOCUMENTATION

Deploying a Quick Template | 515

Quick Templates Overview | 508

CHAPTER 17

Adding and Managing Non Juniper Networks Devices

IN THIS CHAPTER

- Adding Unmanaged Devices | 386
- Modifying Unmanaged Device Configuration | 389

Adding Unmanaged Devices

In the Junos Space Network Management Platform context, unmanaged devices are those made by vendors other than Juniper Networks, Inc. You can add such devices to Junos Space Platform manually, or by importing multiple devices simultaneously from a CSV file.

To add a non-Juniper device to Junos Space Network Management Platform:

1. On the Junos Space Network Management Platform user interface, select **Devices > Unmanaged Devices**.

   The Add Unmanaged Devices page is displayed.

2. You can add non-Juniper devices either manually or using a CSV file. To add the devices manually, select the **Add Manually** option button.

   The Device Details area is displayed on the Add Unmanaged Devices page.

3. Select the **IP Address** or **Hostname** option button.

   If you selected the IP Address option, enter the IP address of the device.

   > **NOTE:** You can enter the IP address in either IPv4 or IPv6 format. Refer to http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml for the list of restricted IPv6 addresses.

   If you selected the Hostname option, enter the hostname of the device.

4. (Optional) In the **Vendor** field, enter the name of the device's vendor.
   The maximum length is 256 characters. Spaces are acceptable.

5. (Optional) Select the **Configure Loopback** check box if you want to configure the loopback address for the device.

   If you do so, the Loopback Settings area appears.

   a. In the **Loopback Name** field, enter the loopback name for the device.

   b. In the **Loopback Address** field, enter the loopback address for the device.

      You can specify both IPv4 and IPv6 addresses as loopback addresses. The valid range for IPv4 loopback address is 1.0.0.1–223.255.255.254. The valid range for IPv6 loopback address is 1::–ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.

6. Select the **Use SNMP** check box to use SNMP to gather device information.
   If you do so, the SNMP Settings area is displayed.

7. Use the option buttons to select either SNMP V1/V2C or SNMP V3.

   - If you select SNMP V1/V2C, the Community field appears. Enter the appropriate SNMP community string (password) to give access to the device.
   - If you select SNMP V3, several fields appear, as described in Table 42. Enter values as appropriate.

   Table 42: SNMP V3 Configuration Parameters

Name	Value
Username	Username previously configured on the device
Authentication type	Algorithm used for authentication: MD5, SHA1, or None. MD5 or SHA1 is used to create a hash of the authentication password. Note that only this password is encrypted, not any other packets transmitted.
Authentication password	Password that authenticates Junos Space Network Management Platform to the device to gain access to it. The password must have at least eight characters and can include alphanumeric and special characters, but not control characters.
Privacy type	Encryption algorithm used to encrypt transmitted packets: AES128, AES192, AES256, DES, or None.
Privacy password	Password that allows reading the transmissions themselves. The password must have at least eight characters.

8. (Optional) To add non-Juniper devices using the CSV file, select the **Import From CSV** option button on the Add Unmanaged Devices page.

9. The **Import** area appears, displaying the following links:
   - View Sample CSV
   - Select a CSV To Upload.

   Clicking **View Sample CSV** displays a CSV file in the format shown in Table 43.

   Table 43: Columns in a Sample CSV File for Importing Unmanaged Devices

Column Heading	Sample Data	Validation
Host Name or IP Address	Sunnyvale_R1	Name: Limit of 256 characters, no spaces. IP address: Dotted decimal notation.
Vendor	ABC	Alphabetic characters only
Device UserName	abcd	No validation from Junos Space Network Management Platform
Device Password	abcd123	No validation from Junos Space Network Management Platform
SNMP Version	SNMP V3	SNMP V3, or SNMP V1 or V2C
Community	N/A (for SNMP V3)	Community string (authentication password) for V2; otherwise, N/A
SNMP Username	abcde	Username for SNMP V3; otherwise, N/A
Authentication Type	MD5	MD5, SHA1, or N/A
Authentication Password	abcde123	Must have at least eight characters and can include alphanumeric and special characters, but not control characters
Privacy Type	DES	DES, AES128, AES192, AES256, or N/A
Privacy Password	abcde123	Must have at least eight characters and can include alphanumeric and special characters, but not control characters; can be the same as the authentication password
Loopback Name	lo0	Loopback name for the device
Loopback Address	127.0.0.1	Loopback address for the device. The loopback address should be a valid IP address in the range of 1.0.0.0 to 223.255.255.255

> **NOTE:** You should enter a valid loopback address or enter “N/A” in the Loopback Address column. If you enter an invalid loopback address or leave the cell empty, the associated unmanaged device is not added to Junos Space Network Management Platform.

10. When you have a complete CSV file, select **Select a CSV To Upload**.

11. Click **Next**.

    The Add Unmanaged Devices page displays the list of unmanaged devices with their details.

12. Click **Finish**.

    You are redirected to the Unmanaged Devices page.

RELATED DOCUMENTATION

- Device Management Overview | **189**
- Modifying Unmanaged Device Configuration | **389**
- Viewing Managed Devices | **194**

Modifying Unmanaged Device Configuration

In the Junos Space Network Management Platform context, unmanaged devices are those made by vendors other than Juniper Networks, Inc. You can add such devices to Junos Space Network Management Platform manually, or by importing multiple devices simultaneously from a CSV file.

To modify the configuration on a non-Juniper device:

1. On the Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed. This page lists the unmanaged devices added to Junos Space Network Management Platform.

2. Right-click the unmanaged device whose configuration you want to modify and select **Device Configuration > Unmanaged Device Configuration**. The Modify Unmanaged Device Configuration page is displayed.

3. Modify the unmanaged device configuration.

4. Click **Save**.

RELATED DOCUMENTATION

Device Management Overview | **189**

Viewing Managed Devices | **194**

CHAPTER 18

Accessing Devices

IN THIS CHAPTER

- Launching a Device's Web User Interface | 391
- Looking Glass Overview | 392
- Executing Commands by Using Looking Glass | 393
- Exporting Looking Glass Results in Junos Space Network Management Platform | 395
- Secure Console Overview | 396
- Connecting to a Device by Using Secure Console | 397
- Configuring SRX Device Clusters in Junos Space using Secure Console | 405

Launching a Device's Web User Interface

The Launch Device Web UI action enables you to access the WebUI of a device to manage it directly. The device should have the required Web UI components installed and enabled (for example, J-web).

Once launched, the Web UI appears either in a new tab in your browser or in a new window. Ensure you enable pop-ups on your browser for the device for which the Web UI is being launched.

To launch a device Web UI:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Right-click the device and select **Device Access > Launch Device WebUI**.

3. Click the **https://ipaddress** link.

   Log in and perform the desired operations, following the instructions for your device.

RELATED DOCUMENTATION

Viewing Managed Devices | 194

Understanding How Junos Space Automatically Resynchronizes Managed Devices | 216

Managing Configuration Files Overview | 938

Looking Glass Overview

You use the Looking Glass feature to view device configurations by executing basic CLI commands on the Junos Space user interface. You can execute these commands on multiple devices and compare the configurations and runtime information in these devices. You can execute the following types of commands by using Looking Glass: **show**, **ping**, **test**, and **traceroute**.

The commands that are supported and stored in the Junos Space Network Management Platform database are displayed on the Looking Glass page. When you type the first few letters of the command, the suggestion list displays the commands that are supported, stored, and begin with the letters that you typed.

If you enter a **show** command and do not find any suggestions on the suggestion list, enter the complete command and click the **Refresh Response** button to execute the command.

> **NOTE:** You cannot execute the following types of command by using Looking Glass: **request**, **monitor**, **op**, **restart**, and **clear**.

With Looking Glass, you can perform the following tasks:

- Select a maximum of ten devices to execute commands.
- View the outputs of the commands that you executed on multiple devices in two formats: Format Text view and Table view. The Format Text view displays the command output in plain-text format. The Table view displays the information in a format that resembles the Device Management page in Junos Space Platform.
- Export the results of the executed command in CSV or DOC format.
- Configure a timeout interval to stop executing commands on some devices that take a long time to respond with results. The results for the devices that allowed the commands to be executed within the timeout interval are displayed. The default timeout interval is 120 seconds. You can modify the **Looking Glass Device response timeout in secs** option on the Modify Application Settings page.

You must have the privileges to use Looking Glass on a device. Without permissions to manage a device, you cannot use Looking Glass on the device.

RELATED DOCUMENTATION

Executing Commands by Using Looking Glass | 393
Exporting Looking Glass Results in Junos Space Network Management Platform | 395

Executing Commands by Using Looking Glass

You use Looking Glass to run some commands on a device from the Junos Space user interface. The following types of commands are supported: **show**, **ping**, **test**, and **traceroute**. If you enter an unsupported command, the following message is displayed: **Looking glass supports only the commands without '|','<' and '>' and starting with ping/show/test/traceroute.**

Before you start executing commands by using Looking Glass, ensure that you have configured the **Looking Glass Device response timeout in secs** option on the Modify Application Settings page. This setting defines the maximum time that Junos Space Network Management Platform waits to collect the command output. The default timeout interval is 120 seconds.

To run a supported command on a device by using Looking Glass:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page that appears lists all the devices that currently exist in the Junos Space Platform database.

2. Select the devices on which you want to run the **show** command and select **Device Operations > Looking Glass** from the Actions menu.

   The Looking Glass page is displayed.

3. (Optional) By default, a green check mark is displayed against all the devices, which indicates that all the devices are selected. To select only a few devices, press the Ctrl key and select the devices by clicking the appropriate device icons.

   A green check mark is displayed against the selected devices.

4. In the **Execute Command** field, enter a command or the first few letters of the command.

   A list of suggestions is displayed. The suggestions include only those commands that are present in the Junos Space Platform database and that can be executed on the devices currently selected.

   Lengthy commands that do not fit in the Execute Command field are truncated and displayed with periods (.); for example **CLI_COMMAND....**

   Mouse over the truncated view of the command to view the full command.

> **NOTE:** If the command that you are running requires your input, replace the part of the command shown as text in angle brackets with your own data. For example, replace **<slot>** in **show chassis routing-engine <slot>** with the slot number, as in **show chassis routing-engine 1**.

You can also select a command from the list of commands in this field.

5. (Optional) If you typed the entire command or selected a command from the list, click **Refresh Response** or press Enter.

   The command is executed on the devices. A progress bar indicates that the command is being executed.

   When the command execution is complete, the results are displayed below the Execute Command field. The command that you entered or selected is displayed beside the Refresh Response button. The output of the command executed on these devices is displayed one below the other. Scroll the results to view the output from these devices.

   > **NOTE:** If one of the devices on which you executed the command takes too long to respond with results, the results from this device are omitted and a **Request timeout** message is displayed in a dialog box. The command output for other devices on which the command is successfully executed is displayed.

6. (Optional) The Format Text view is the default view of the output. To change the view of the output, click the Table view icon.

7. (Optional) To view the output for a subset of devices, press the Ctrl key and select the devices whose output you want to view by clicking the appropriate device icons.

8. Click **OK** to exit the Looking Glass page.

   An audit log entry is generated for this task.

RELATED DOCUMENTATION

Looking Glass Overview | 392

Exporting Looking Glass Results in Junos Space Network Management Platform | 395

Exporting Looking Glass Results in Junos Space Network Management Platform

You export Looking Glass results to save the output of the commands you executed by using Looking Glass. You can export the results in Format Text or Table View to your local computer. The ZIP file contains device-specific CSV or DOC files. If you export the results in Format Text view, device-specific DOC files are downloaded. If you export the results in Table view, device-specific CSV files are downloaded.

To export Looking Glass results:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page that appears lists all devices that currently exist in the Junos Space Platform database.

2. Select the devices on which you want to run the **show** command and select **Device Operations > Looking Glass** from the Actions menu.

   The Looking Glass page is displayed.

3. In the **Execute Command** field, enter a command or the first few letters of the command.

   A list of suggestions is displayed. The suggestions include only those commands that are present in the Junos Space Platform database and that can be executed on the devices currently selected.

   You can also select a command from the list of commands in this field.

4. (Optional) If you typed the entire command or selected a command from the list, click **Refresh Response** or press Enter.

   The command is executed on the devices. A progress bar indicates that the command is being executed.

   When the command execution is complete, the results are displayed below the Execute Command field. The output of the command executed on these devices is displayed one below the other. Scroll the results to view the output from these devices.

5. To select the view that you want to export, click the appropriate icon: Format Text view or Table view.

   By default the results are displayed in the Format Text view.

6. Click the Export Results icon.

   The Export Results dialog box is displayed.

> **NOTE:** The icon appears dimmed if the results are not displayed when you execute the command.

7. Click **OK** and save the ZIP file to your local computer.

   The ZIP file contains device-specific CSV or DOC files with the command output. To help you identify the files easily, the files are named after the device.

Click **OK** to exit the Looking Glass page.

An audit log is generated for this task.

RELATED DOCUMENTATION

Looking Glass Overview | 392

Executing Commands by Using Looking Glass | 393

Secure Console Overview

The Secure Console feature provides a secure remote access connection to managed and unmanaged devices. Secure Console initiates an SSH session from the Junos Space user interface by using the SSH protocol. An unmanaged device is a device that is not managed by Junos Space Network Management Platform.

Secure Console is a terminal window embedded in Junos Space Platform that eliminates the need for a third-party SSH client to connect to devices. Secure Console provides additional security while connecting to your devices. It initiates an SSH session from the Junos Space server rather than from your Web browser. You can access the Secure Console feature either from the Device Management page or the Secure Console page.

When using Secure Console for a managed device, you can skip the steps to log in to the device by selecting the **Allow users to auto log in to devices using SSH** option on the Modify Application settings page. If you select this option, you are automatically logged in to the device. However, for an unmanaged device, you need to provide the device credentials manually.

Secure Console provides the following functionalities:

- Validate the fingerprint value stored in the Junos Space Platform database with that obtained from the device.
- Establish multiple SSH connections to connect to different devices simultaneously. These multiple connections are displayed in different terminal windows.
- Compare configurations on a device by establishing multiple SSH connections to the same device and viewing the configurations in different SSH terminal windows.
- Resize the terminal windows to a desired size.
- Minimize the terminal windows to the taskbar and maximize them.
- Paste the CLI commands into the terminal window.
- Terminal windows allow the use of the following terminal control characters: **CRTL** + **A**, **CRTL**+ **E**, ↑, and **TAB**.

> **NOTE:** The SSH session is terminated if:
>
> - You are logged out due to inactivity.
> - Your user account is terminated, disabled, or deleted.
> - The authentication mode is switched to Certificate mode.
> - If the Manually Resolve Fingerprint Conflict check box on the Modify Application Settings page in the Administration workspace is enabled, and Junos Space Platform detects a conflict between the fingerprint stored in the database and that received from the device.

You must have the privileges of a Super Administrator or a Device Manager to use the Secure Console feature and connect to devices.

RELATED DOCUMENTATION

Connecting to a Device by Using Secure Console | 397

Connecting to a Device by Using Secure Console

You use Secure Console to establish an SSH connection to a device from the Junos Space user interface. You can establish multiple SSH connections and connect to multiple managed or unmanaged devices. You

can also establish multiple SSH sessions to the same device. A new SSH terminal window is opened for every new connection to the device.

CAUTION: Some browser plug-ins may cause undesirable behavior in open SSH windows; disabling such plug-ins may resolve the issue. For example, if the Firebug plug-in is activated within an SSH window opened in Mozilla Firefox, the window cannot be restored, resized, or maximized and the console area remains fixed; disabling the Firebug plug-in resolves this issue.

You can connect to a device through an SSH connection from the Device Management page or the Secure Console page.

This topic includes steps to connect to a managed and unmanaged device from the Device Management or Secure Console page.

- Connecting to a Managed Device from the Device Management Page | **398**
- Connecting to an Unmanaged Device from the Device Management Page | **401**
- Connecting to a Managed or Unmanaged Device from the Secure Console Page | **403**

Connecting to a Managed Device from the Device Management Page

Before you open an SSH session to connect to a managed device from the Device Management page, ensure that:

- You have the privileges of a Super Administrator or Device Manager in Junos Space Network Management Platform.
- The status of the managed device is “UP.”
- You have configured the **Allow users to auto log in to devices using SSH** option on the Modify Applications page. If you select this option, Junos Space Platform automatically logs in to the device when an SSH connection is initiated to the device.

  To connect to a logical system, you must always enter the username and password irrespective of whether or not you have selected the **Allow users to auto log in to devices using SSH** option.

To connect to a managed device:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Select a device to which you want to connect and select **Device Access > SSH to Device** from the Actions menu.

   The SSH to Device pop-up window is displayed.

   > **NOTE:** If you have cleared the **Allow users to auto log in to devices using SSH** option on the Modify Applications page, the SSH to Device pop-up window is displayed. The IP address is automatically displayed in the IP address field. Enter the username and password in the **User name** and **Password** fields respectively.

3. In the **IP Address** field, enter a valid IP address of the device.

   > **NOTE:** You can enter the IP address in either the IPv4 or IPv6 format. Refer to http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml for a list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml for a list of restricted IPv6 addresses.

4. In the **Username** field, enter the username of the device.

   The username must match the username configured on the device.

5. In the **Password** field, enter the password to access the device.

   The password must match the password configured on the device.

6. If you want to change the value, specify a value specified in the SSH port for device connection field on the Modify Application Settings page in the Administration workspace

   The default value is 22.

   > **NOTE:** If you enter a port number other than the one you specified on the Modify Application Settings page, the SSH connection is not established.

7. Click **Connect**.

   Junos Space Platform validates the fingerprint stored in the database with that on the device.

   - If you have enabled the Manually Resolve Fingerprint Conflict check box on the Modify Application Settings page in the Administration workspace and the fingerprints do not match, the connection is disconnected and the Device Authenticity error message dialog box is displayed. The authentication status of the device is modified to Fingerprint Conflict.
   - If you have disabled the Manually Resolve Fingerprint Conflict check box on the Modify Application Settings page in the Administration workspace and the fingerprints do not match, the new fingerprint is updated in the Junos Space Platform database.

   If the fingerprints on the device match the fingerprints in the database, the SSH terminal window is displayed.

   > **NOTE:** You may receive error messages such as **Unable to Connect**, **Authentication Error**, or **Connection Lost or Terminated**, which are displayed as standard text in the terminal window. If you receive an error message, all other functionality in the terminal window is stopped. You should close this terminal window and open a new SSH session.

8. You can perform the following tasks in the terminal window:

   - (Optional) Enter CLI commands to monitor and troubleshoot the device from this terminal window. Use the following terminal control characters:
     - **Ctrl+a**—Moves the cursor to the start of the command line
     - **Ctrl+e**—Moves the cursor to the end of the command line
     - ↑ (Up arrow key)—Repeats the previous command
     - **Tab**—Completes a partially typed command
   - (Optional) Minimize or maximize the terminal window by clicking the minimize or maximize button on the top-right corner.
   - (Optional) Resize the terminal window by dragging the terminal window horizontally or vertically by using the mouse.
   - (Optional) Terminate a process by using the **Ctrl+c** key combination.
   - (Optional) Right-click the terminal window to copy and paste the command from the local computer.
   - To terminate the SSH session, type **exit** and press Enter.

Click **Close** to close the SSH terminal window.

Connecting to an Unmanaged Device from the Device Management Page

Before you connect to an unmanaged device by using the Secure Console from the Device Management page, ensure that:

- You have the privileges of a Super Administrator or Device Manager in Junos Space Network Management Platform.
- The device is configured with a static management IP address. This IP address should be reachable from the Junos Space Appliance.
- The SSH v2 protocol is enabled on the device.

  To enable SSH v2 on a device, enter the **set system services ssh protocol-version v2** command at the command prompt.
- The status of the device is "UP."
- A valid username and password are created on the device.
- Clear the **Allow users to auto log in to devices using SSH** option on the Modify Application Settings page.

To connect to an unmanaged device:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Select the unmanaged device and select **Device Access > SSH to Device** from the Actions menu.

   The SSH to Device pop-up window is displayed.

3. In the **IP Address** field, enter a valid IP address for the device.

   NOTE: You can enter the IP address in either the IPv4 or IPv6 format. Refer to http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml for a list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml for a list of restricted IPv6 addresses.

4. In the **Username** field, enter the username for the device.

   The username must match the username configured on the device.

5. In the **Password** field, enter the password to access the device.

The password must match the password configured on the device.

6. In the **Port** field, enter the port number to use for the SSH connection.

   The default value is 22. If you want to change the value, specify a value specified in the SSH port for device connection field on the Modify Application Settings page in the Administration workspace.

7. Click **Connect**.

   The Device Authenticity dialog box is displayed. This dialog box displays the SSH fingerprint of the unmanaged device.

8. Click **Yes**.

   The SSH terminal window is displayed.

   > **NOTE:** You may receive error messages such as **Unable to Connect**, **Authentication Error**, or **Connection Lost or Terminated**, which are displayed as standard text in the terminal window. If you receive an error message, all other functionality in the terminal window is stopped. You should close this terminal window and open a new SSH session.

9. You can perform the following tasks in the terminal window:

   - (Optional) Enter CLI commands to monitor and troubleshoot the device from this terminal window. Use the following terminal control characters:
     - **Ctrl+a** —Moves the cursor to the start of the command line
     - **Ctrl+e**—Moves the cursor to the end of the command line
     - ↑ (Up arrow key)—Repeats the previous command
     - **Tab**—Completes a partially typed command
   - (Optional) Minimize or maximize the terminal window by clicking the minimize or maximize button on the top-right corner.
   - (Optional) Resize the terminal window by dragging the terminal window horizontally or vertically by using the mouse.
   - (Optional) Terminate a process by using the **Ctrl+c** key combination.
   - (Optional) Right-click the terminal window to copy and paste the command from the local computer.
   - To terminate the SSH session, type **exit** and press Enter.

Click **Close** to close the SSH terminal window.

Connecting to a Managed or Unmanaged Device from the Secure Console Page

Before you connect to a managed or unmanaged device from the Secure Console page, ensure that:

- You have the privileges of a Super Administrator or Device Manager in Junos Space Network Management Platform.
- The device is configured with a static management IP address. This IP address should be reachable from the Junos Space Appliance.
- The SSH v2 protocol is enabled on the device.

  To enable SSH v2 on a device, enter the **set system services ssh protocol-version v2** command at the command prompt.
- The status of the device is “UP.”
- A valid username and password are created on the device.

To connect to a managed or unmanaged device from the Secure Console page:

1. On the Junos Space Network Management Platform user interface, select **Devices > Secure Console**.

   The Secure Console page is displayed. This page displays the fields you need to specify to connect using the Secure Console.

2. In the **Username** field, enter the username of the device.

   The username must match the username configured on the device.

3. In the **Password** field, enter the password to access the device.

   The password must match the password configured on the device.

4. If you want to change the value, specify a value specified in the SSH port for device connection field on the Modify Application Settings page in the Administration workspace.

   The default value is 22.

5. Click **Connect**.

   If you are connecting to a Juniper Networks device, Junos Space Platform validates the fingerprint stored in the database with that on the device.

   - If you have enabled the Manually Resolve Fingerprint Conflict check box on the Modify Application Settings page in the Administration workspace and the fingerprints do not match, the connection is disconnected and the Device Authenticity error message dialog box is displayed. The authentication status of the device is modified to Fingerprint Conflict.

- If you have disabled the Manually Resolve Fingerprint Conflict check box on the Modify Application Settings page in the Administration workspace and the fingerprints do not match, the new fingerprint is updated in the Junos Space Platform database.

If the fingerprints on the device match the fingerprints in the database, the SSH terminal window is displayed.

If you are connecting to an unmanaged device, the Device Authenticity error message dialog box is displayed. This dialog box displays the SSH fingerprint of the unmanaged device.

a. Click **Yes**.

The SSH terminal window is displayed.

> **NOTE:** You may receive error messages such as **Unable to Connect**, **Authentication Error**, or **Connection Lost or Terminated**, which are displayed as standard text in the terminal window. If you receive an error message, all other functionality in the terminal window is stopped. You should close this terminal window and open a new SSH session.

6. You can perform the following tasks in the terminal window:
   - (Optional) Enter CLI commands to monitor and troubleshoot the device from this terminal window. Use the following terminal control characters:
     - **Ctrl+a**—Moves the cursor to the start of the command line
     - **Ctrl+e**—Moves the cursor to the end of the command line
     - ↑ (up arrow key)—Repeats the previous command
     - **Tab**—Completes a partially typed command
   - (Optional) Minimize or maximize the terminal window by clicking the minimize or maximize button on the top-right corner.
   - (Optional) Resize the terminal window by dragging the terminal window horizontally or vertically by using the mouse.
   - (Optional) Terminate a process using the **Ctrl+c** key combination.
   - (Optional) Right-click the terminal window to copy and paste the command from the local computer.
   - To terminate the SSH session, type **exit** and press Enter.

Click **Close** to close the SSH terminal window.

RELATED DOCUMENTATION

Secure Console Overview | 396

Configuring SRX Device Clusters in Junos Space using Secure Console

You can create a cluster of two SRX-series devices that are combined to act as a single system, or create a single-device cluster and then add a second device to the cluster later. You can also configure a standalone device from an existing cluster device. You can do this using the Secure Console feature in the Devices workspace.

You can configure an SRX-series cluster in the following modes:

- Active/passive clustering
- Active/active clustering

In the active/passive mode, the transit traffic passes through the primary node, while the backup node is used only in the event of a failure. When failure occurs, the backup device becomes the primary and takes over all the forwarding tasks.

In the active/active mode, the transit traffic always passes through both the nodes of the cluster.

NOTE: To discover and manage an SRX device cluster that is already configured, you must perform the device discovery workflow independently for each cluster node. You can add and discover the cluster devices using the Web UI. The discovery process is common for both standalone devices and cluster devices. For more information, see "Running Device Discovery Profiles" on page 238.

This topic includes the following tasks:

- Configuring a Standalone Device from a Single-node Cluster | 405
- Configuring a Standalone Device from a Two-Node Cluster | 408
- Configuring a Primary Peer in a Cluster from a Standalone Device | 410
- Configuring a Secondary Peer in a Cluster from a Standalone Device | 413
- Configuring a Cluster with Loopback Interface | 415

Configuring a Standalone Device from a Single-node Cluster

You can configure a standalone device from device that is currently configured as a single-node cluster.

To configure a single-node cluster as a standalone device:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

2. Select the single-node cluster and select **Device Access > SSH to Device** from the Actions menu.

   The SSH to Device pop-up window is displayed.

   > **NOTE:** If you have cleared the **Allow users to auto log in to devices using SSH** option on the Modify Applications page, the SSH to Device pop-up window is displayed. The IP address is automatically displayed in the IP address field. Enter the username and password in the **User name** and **Password** fields respectively.

3. In the **IP Address** field, enter a valid IP address for the device.

4. In the **Username** field, enter the user name for the device.

5. In the **Password** field, enter the password to access the device.

   The name and password must match the name and password configured on the device.

6. In the **Port** field, enter the port number to use for the SSH connection.

   The default value is 22. If you want to change the value, specify a value specified in the SSH port for device connection field on the Modify Application Settings page in the Administration workspace.

7. Click **Connect**.

   The SSH terminal window is displayed.

   > **NOTE:** You may receive error messages such as “Unable to Connect”, “Authentication Error”, or “Connection Lost or Terminated”, which are displayed as standard text in terminal window. If you receive an error message, all other functionality in the terminal window is stopped. You should close this terminal window and open a new SSH session.

8. Enter the set chassis command to remove the cluster configuration:

   set chassis cluster cluster-id 0 node 0

9. Reboot the device, by entering the command:

request system reboot

10. Copy the outbound-ssh configuration from group node to system level, for example:

    set system services outbound-ssh client 00089BBC494A device-id 6CFF68

    set system services outbound-ssh client 00089BBC494A secret "$ABC123"

    set system services outbound-ssh client 00089BBC494A services netconf

    set system services outbound-ssh client 00089BBC494A 10.155.70.252 port 7804

11. Copy the system log configuration from group node to system level:

    set system syslog file default-log-messages any any

    set system syslog file default-log-messages structured-data

12. Copy the fxp0 interface setting from group node to system level, for example:

    set interfaces fxp0 unit 0 family inet address 10.155.70.223/19

13. Delete the outbound-ssh configuration from the group node, for example:

    delete groups node0 system services outbound-ssh

14. Delete the system log configuration from the group node, for example:

    delete groups node0 system syslog file default-log-messages any any

    delete groups node0 system syslog file default-log-messages structured-data

15. Delete the interfaces configuration from the group node, for example:

    delete groups node0 interfaces fxp0 unit 0 family inet address 10.155.70.223/19

16. Commit the configuration changes on the device:

    commit

    In the Junos Space user interface, the device connection status will go down and then up again. After the device connection is back up, you can verify that the device you configured displays as a standalone device.

17. To terminate the SSH session, type **exit** from the terminal window prompt, and press Enter.

18. Click in the top right corner of the terminal window to close the window.

Configuring a Standalone Device from a Two-Node Cluster

You can configure a standalone device from the secondary peer device in a cluster.

> **NOTE:** You cannot use the primary peer in a two-node cluster to configure a standalone device.

To configure a secondary peer device in a cluster as a standalone device:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

2. Select the secondary peer device and select **Device Access > SSH to Device** from the Actions menu.

   The SSH to Device pop-up window is displayed.

3. Select the single-node cluster and select **Device Access > SSH to Device** from the Actions menu.

   The SSH to Device pop-up window is displayed.

   > **NOTE:** If you have cleared the **Allow users to auto log in to devices using SSH** option on the Modify Applications page, the SSH to Device pop-up window is displayed. The IP address is automatically displayed in the IP address field. Enter the username and password in the **User name** and **Password** fields respectively.

4. In the **IP Address** field, enter a valid IP address for the device.

5. In the **Username** field, enter the user name for the device.

6. In the **Password** field, enter the password to access the device.

   The name and password must match the name and password configured on the device.

7. In the **Port** field, enter the port number to use for the SSH connection.

   The default value is 22. If you want to change the value, specify a value specified in the SSH port for device connection field on the Modify Application Settings page in the Administration workspace.

8. Click **Connect**.

   The SSH terminal window is displayed.

   > **NOTE:** You may receive error messages such as “Unable to Connect”, “Authentication Error”, or “Connection Lost or Terminated”, which are displayed as standard text in terminal window. If you receive an error message, all other functionality in the terminal window is stopped. You should close this terminal window and open a new SSH session.

9. Disconnect the HA cable from the device that you want to configure as a standalone device.

10. Enter the set chassis command for the peer device, for example:

    set chassis cluster cluster-id 0 node 1

11. Reboot the device, by entering the command:

    request system reboot

12. Copy the outbound-ssh configuration from group level to system level, for example:

    set system services outbound-ssh client 00089BBC494A device-id 6CFF68

    set system services outbound-ssh client 00089BBC494A secret "$ABC123"

    set system services outbound-ssh client 00089BBC494A services netconf

    set system services outbound-ssh client 00089BBC494A 10.155.70.252 port 7804

13. Copy the system log configuration from group level to system level:

    set system syslog file default-log-messages any any

    set system syslog file default-log-messages structured-data

14. Copy the fxp0 interface setting from group level to system level, for example:

    set interfaces fxp0 unit 0 family inet address 10.155.70.223/19

15. Delete the outbound-ssh configuration from the group level, for example:

    delete groups node1 system services outbound-ssh

16. Delete the system log configuration from the group level, for example:

delete groups node1 system syslog file default-log-messages any any

delete groups node1 system syslog file default-log-messages structured-data

17. Delete the interfaces configuration from the group level, for example:

    delete groups node1 interfaces fxp0 unit 0 family inet address 10.155.70.223/19

18. Commit the configuration changes on the device:

    commit

    In the Junos Space user interface, the device connection status will go down and then up again. After the device connection is back up, you can verify that the device you configured displays as a standalone device.

    After the device connections are up, verify the following changes in the Manage Devices inventory landing page:

    - The device you configured now displays as a standalone device.
    - The cluster that formerly included a primary and secondary peer device now displays the primary peer device only.

19. To terminate the SSH session, type **exit** from the terminal window prompt, and press Enter.

20. Click in the top right corner of the terminal window to close the window.

Configuring a Primary Peer in a Cluster from a Standalone Device

You can create a device cluster from two standalone devices. Use the following procedure to configure a standalone device as the primary peer in a cluster.

To configure a primary peer in a cluster from a standalone device:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

2. Select the primary peer in the cluster and select **Device Access > SSH to Device** from the Actions menu.

   The SSH to Device pop-up window is displayed.

> **NOTE:** If you have cleared the **Allow users to auto log in to devices using SSH** option on the Modify Applications page, the SSH to Device pop-up window is displayed. The IP address is automatically displayed in the IP address field. Enter the username and password in the **User name** and **Password** fields respectively.

3. In the **IP Address** field, enter a valid IP address for the device.
4. In the **Username** field, enter the user name for the device.
5. In the **Password** field, enter the password to access the device.

   The name and password must match the name and password configured on the device.
6. In the **Port** field, enter the port number to use for the SSH connection.

   The default value is 22. If you want to change the value, specify a value specified in the SSH port for device connection field on the Modify Application Settings page in the Administration workspace.
7. Click **Connect**.

   The SSH terminal window is displayed.

   > **NOTE:** You may receive error messages such as “Unable to Connect”, “Authentication Error”, or “Connection Lost or Terminated”, which are displayed as standard text in terminal window. If you receive an error message, all other functionality in the terminal window is stopped. You should close this terminal window and open a new SSH session.

8. For the standalone device, enter the command:

   set chassis cluster cluster-id 1 node 0
9. Reboot the device, by entering the command:

   request system reboot
10. Copy the outbound-ssh configuration from the system level to the group level, for example:

    set groups node0 system services outbound-ssh client 00089BBC494A device-id 6CFF68

    set groups node0 system services outbound-ssh client 00089BBC494A secret "$ABC123"

set groups node0 system services outbound-ssh client 00089BBC494A services netconf

set groups node0 system services outbound-ssh client 00089BBC494A 10.155.70.252 port 7804

11. Copy the fxp0 interface configuration from the system level to the group level, for example:

    set groups node0 interfaces fxp0 unit 0 family inet address 10.155.70.223/19

12. Copy the system log configuration from system level to group level:

    set groups node0 system syslog file default-log-messages any any

    set groups node0 system syslog file default-log-messages structured-data

13. Delete the outbound-ssh configuration from the system level, for example:

    delete system services outbound-ssh

14. Delete the system log configuration from the system level, for example:

    delete system syslog file default-log-messages any any

    delete system syslog file default-log-messages structured-data

15. Delete the interfaces configuration from the system level, for example:

    delete interfaces fxp0 unit 0 family inet address 10.155.70.223/19

16. Commit the configuration changes on the device again:

    commit

    After the device connection is up, verify the following changes:

    - In the Manage Devices inventory landing page:
      - The cluster icon appears for the device.
      - The new cluster device appears as the primary device.
    - In the physical inventory landing page, Junos Space Network Management Platform displays chassis information for the primary device cluster.

17. To terminate the SSH session, type **exit** from the terminal window prompt, and press Enter.

18. Click in the top right corner of the terminal window to close the window.

Configuring a Secondary Peer in a Cluster from a Standalone Device

If a device cluster contains only a primary peer, you can configure a standalone device to function as a secondary peer in the cluster. Use the following procedure to ensure that Junos Space Network Management Platform is able to manage both devices.

To add a standalone device to a cluster:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

2. Select the device and select **Device Access > SSH to Device** from the Actions menu.

   The SSH to Device pop-up window is displayed.

   > **NOTE:** If you have cleared the **Allow users to auto log in to devices using SSH** option on the Modify Applications page, the SSH to Device pop-up window is displayed. The IP address is automatically displayed in the IP address field. Enter the username and password in the **User name** and **Password** fields respectively.

3. In the **IP Address** field, enter a valid IP address for the device.

4. In the **Username** field, enter the user name for the device.

5. In the **Password** field, enter the password to access the device.

   The name and password must match the name and password configured on the device.

6. In the **Port** field, enter the port number to use for the SSH connection.

   The default value is 22. If you want to change the value, specify a value specified in the SSH port for device connection field on the Modify Application Settings page in the Administration workspace.

7. Click **Connect**.

   The SSH terminal window is displayed.

   From the terminal window prompt, you can enter CLI commands to create a standalone device from the device cluster.

> **NOTE:** You may receive error messages such as “Unable to Connect”, “Authentication Error”, or “Connection Lost or Terminated”, which are displayed as standard text in terminal window. If you receive an error message, all other functionality in the terminal window is stopped. You should close this terminal window and open a new SSH session.

8. For the standalone device, enter the command:

   set chassis cluster cluster-id 1 node 1

9. Enter the command:

   request system reboot

10. Copy the outbound-ssh configuration from the system level to the group level, for example:

    set groups node1 system services outbound-ssh client 00089BBC494A device-id 6CFF68

    set groups node1 system services outbound-ssh client 00089BBC494A secret "$ABC123"

    set groups node1 system services outbound-ssh client 00089BBC494A services netconf

    set groups node1 system services outbound-ssh client 00089BBC494A 10.155.70.252 port 7804

11. Copy the fxp0 interface configuration from the system level to the group level, for example:

    set groups node1 interfaces fxp0 unit 0 family inet address 10.155.70.223/19

12. Copy the system log configuration from system level to group level:

    set groups node1 system syslog file default-log-messages any any

    set groups node1 system syslog file default-log-messages structured-data

13. Delete the outbound-ssh configuration from the system level, for example:

    delete system services outbound-ssh

14. Delete the system log configuration from the system level, for example:

    delete system syslog file default-log-messages any any

    delete system syslog file default-log-messages structured-data

15. Delete the interfaces configuration from the system level, for example:

    delete interfaces fxp0 unit 0 family inet address 10.155.70.223/19

16. Commit the configuration changes on the device again:

    commit

17. Connect the HA cable to each device in the cluster.

18. Establish an SSH connection to the primary device in the cluster.

19. On the primary device, make some trivial change to the device, for example, add a description, and commit the change:

    commit

    After the device connections are up for both devices in the cluster, verify the following changes:

    - In the Manage Devices inventory landing page:
      - Each peer device displays the other cluster member.
      - The cluster icon appears for each member device.
      - One device appears as the primary device and the other as the secondary device in the cluster.
    - In the physical inventory landing page, chassis information appears for each peer device in the cluster.

20. To terminate the SSH sessions, type **exit** from the terminal window prompt, and press Enter.

21. Click in the top right corner of the terminal window to close the window.

Configuring a Cluster with Loopback Interface

By default, the SRX devices are configured to be managed through the fxp0 Ethernet management interface.

If the device is managed through non-fxp0 interface (loopback address), add the following additional command to the device so that the SRX device is considered as a cluster in Junos Space:

Command: **set chassis cluster network-management cluster-master**

> **NOTE:** All other cluster configuration commands remain the same for both the Active/Active mode, and Active/Passive mode.

RELATED DOCUMENTATION

Secure Console Overview | 396

Connecting to a Device by Using Secure Console | 397

Example: Configuring an Active/Active Layer 3 Cluster Deployment

Example: Configuring an Active/Passive Cluster Deployment

CHAPTER 19

Logical Systems (LSYS)

IN THIS CHAPTER

- Understanding Logical Systems for SRX Series Services Gateways | 417
- Creating a Logical System (LSYS) | 418
- Deleting Logical Systems | 419
- Viewing Logical Systems for a Physical Device | 420
- Viewing the Physical Device for a Logical System | 420

Understanding Logical Systems for SRX Series Services Gateways

Logical systems for SRX Series devices enable you to partition a single device into secure contexts. Each logical system has its own discrete administrative domain, logical interfaces, routing instances, security firewall and other security features. By transforming an SRX Series device into a multitenant logical systems device, you can give various departments, organizations, customers, and partners–depending on your environment–private use of portions of its resources and a private view of the device. Using logical systems, you can share system and underlying physical machine resources among discrete user logical systems and the primary logical system. The logical systems feature runs with the Junos operating system (Junos OS) on SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices.

For detailed information about understanding and configuring logical systems for SRX series services gateways, see *Junos OS Logical Systems Configuration Guide for Security Devices*

RELATED DOCUMENTATION

- Viewing the Physical Device for a Logical System | 420
- Viewing Logical Systems for a Physical Device | 420
- Creating a Logical System (LSYS) | 418
- Deleting Logical Systems | 419

Creating a Logical System (LSYS)

Logical systems for SRX Series devices enable you to partition a single device into secure contexts. Each logical system has its own discrete administrative domain, logical interfaces, routing instances, security firewall and other security features.

> **NOTE:** You must create a LSYS profile on the device before creating a logical system. To create a LSYS profile on a device from Junos Space Platform, deploy the configuration to create a LSYS profile by using Junos Space Platform features such as device templates or CLI Configlets. To create a LSYS profile by using the Quick Templates feature, see "Creating a Quick Template" on page 509 and "Deploying a Quick Template" on page 515.

For detailed information about using logical systems on Juniper Networks security devices, see *Junos OS Logical Systems Configuration Guide for Security Devices*.

To create a new logical system on a physical device:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page appears.

2. Select a device for which you want to create a logical system and then select **Device Operations > Create LSYS** from the Actions menu.

   The New Logical System pop-up window is displayed.

3. In the **LSYS device name** field, enter a user-defined name for the new logical system.

4. From the **LSYS profile** drop-down list, choose a logical system security profile for the new logical system.

   > **NOTE:** If you have not created a LSYS profile on the device, the drop-down list will not display any LSYS profiles.

5. Click **Finish** to create the new logical system.

RELATED DOCUMENTATION

Understanding Logical Systems for SRX Series Services Gateways | 417
Viewing Devices and Logical Systems with QuickView | 447
Viewing the Physical Device for a Logical System | 420
Viewing Logical Systems for a Physical Device | 420
Deleting Logical Systems | 419

Deleting Logical Systems

For detailed information about using logical systems on Juniper Networks security devices, see *Junos OS Logical Systems Configuration Guide for Security Devices*

> **NOTE:** We recommend that you *not* delete an SRX root device and an LSYS simultaneously in Junos Space Network Management Platform. Although deleting the SRX root device will delete the root device and the LSYS instances from Junos Space Network Management Platform, it will not remove the LSYS configuration from the device, whereas deleting an LSYS will remove LSYS-related configuration from the device.

To delete logical systems:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Select a logical system and select **Device Operations > Delete Devices** from the Actions menu.

   The Delete Logical Systems pop-up window is displayed.

3. Click **Confirm** to proceed with the deletion of the logical systems.

RELATED DOCUMENTATION

Understanding Logical Systems for SRX Series Services Gateways | 417
Viewing Devices and Logical Systems with QuickView | 447
Viewing the Physical Device for a Logical System | 420
Viewing Logical Systems for a Physical Device | 420
Creating a Logical System (LSYS) | 418

Viewing Logical Systems for a Physical Device

For detailed information about using logical systems on Juniper Networks security devices, see *Junos OS Logical Systems Configuration Guide for Security Devices*

To view the logical systems configured on a selected physical device:

1. Select **Devices > Device Management**.

2. On the Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page displays the devices managed in Junos Space Network Management Platform.

3. Locate the table row for the physical device.

   If the device supports logical systems, the device name will be followed by link text indicating how many logical systems are configured on it. If no logical systems are configured on the device, the link text reads “0 LSYS(s).”

4. Click on the link text next to the name of the physical device.

   Space Platform filters the device inventory list so that it lists the logical systems configured on the selected physical device.

5. To clear the filter and return the inventory list to its original view, click the red X next to the filter criteria above the inventory list.

RELATED DOCUMENTATION

- Understanding Logical Systems for SRX Series Services Gateways | **417**
- Viewing Devices and Logical Systems with QuickView | **447**
- Viewing the Physical Device for a Logical System | **420**
- Creating a Logical System (LSYS) | **418**
- Deleting Logical Systems | **419**

Viewing the Physical Device for a Logical System

For detailed information about using logical systems on Juniper Networks security devices, see *Junos OS Logical Systems Configuration Guide for Security Devices*

To view the physical device on which a selected logical system is configured:

1. On the Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page displays the devices managed in Junos Space Network Management Platform.

2. In the tabular view, locate the table row for the logical system.

   The logical system name will be followed by link text indicating the name of the physical device on which the logical system is configured.

3. Click on the link text next to the name of the logical system.

   Space Platform filters the device inventory list so that it shows only the entry for the physical device on which the logical system is configured.

4. To clear the filter and return the inventory list to its original view, click the red X next to the filter criteria above the inventory list.

RELATED DOCUMENTATION

- Understanding Logical Systems for SRX Series Services Gateways | **417**
- Viewing Devices and Logical Systems with QuickView | **447**
- Viewing Logical Systems for a Physical Device | **420**
- Creating a Logical System (LSYS) | **418**
- Deleting Logical Systems | **419**

CHAPTER 20

Device Partitions

IN THIS CHAPTER

- Creating Device Partitions | 422
- Modifying Device Partitions | 423
- Deleting Device Partitions | 424

Creating Device Partitions

Create device partitions when you want to share the physical interfaces, logical interfaces, and physical inventory elements across multiple sub-domains. Device partitions are supported only on M Series and MX Series routers. You can partition a device from the Device Management workspace. You can assign only one partition from a device to a sub-domain; you cannot assign multiple partitions from the same device to a sub-domain. A maximum of one partition can be assigned from multiple devices to a sub-domain. You can partition a device only if the device is currently assigned to the global domain. For more information, see “Working with Domains” on page 1085.

To create a device partition:

1. On the Junos Space Network Management Platform user interface, select **Device > Device Management.**

   The Device Management page is displayed.

2. Select the device that you want to partition and select **Device Operations > Manage Device Partitions** from the Actions menu.

   The Manage Device Partitions page is displayed.

3. Click the Create Partition icon from the Actions menu.

   The Create Partition page is displayed. You can view the physical interfaces, logical interfaces, and the physical inventory of the device.

4. In the **Partition Name** field, enter a name for the partition.

5. Select the **Physical Interface** tab and select the physical interfaces that you want to add to the partition.

You can view the selected physical interfaces in the Selected Sub-object section.

6. Select the **Logical Interface** tab and select the logical interfaces that you want to add to this partition.

   You can view the selected logical interfaces in the Selected Sub-object section.

7. Select the **Physical Inventory** tab and select the inventory elements that you want to add to this partition.

   You can view the selected inventory elements such as FPCs, and Routing Engines in the Selected Sub-object section.

8. Click **OK**.

   The new device partition is created.Repeat steps 3 through 8 to add multiple device partitions. You can now assign this partition to a sub-domain.

> **NOTE:** When you create the second device partition, the physical interfaces, logical interfaces, and physical inventory elements that you assigned to the first device partition are not available for selection.

RELATED DOCUMENTATION

Modifying Device Partitions | 423

Modifying Device Partitions

You can modify device partitions from the Devices workspace. The device partitions are listed on the Device Management page.

To modify device partitions:

1. On the Junos Space Network Management Platform user interface, select **Device > Device Management.**

   The Device Management page is displayed. You can view the devices and the device partitions on this page.

2. Select the device whose device partitions you want to modify and select **Device Operations > Manage Device Partitions** from the Actions menu.

The Manage Device Partitions page is displayed.

3. Select the device partition you want to modify and click the Modify Partition icon on the Actions menu.

   The Modify Partition page is displayed.

4. Modify the physical interfaces, logical interfaces, and physical inventory elements for this device partition. You cannot modify the name of the partition.

5. Click **OK**.

6. Repeat steps 3 through 5 to modify any other device partitions.

   The device partitions are modified.

RELATED DOCUMENTATION

Domains Overview | 1077
Creating Device Partitions | 422
Deleting Device Partitions | 424

Deleting Device Partitions

You can delete the device partitions on a device from the Devices workspace. The device partitions are listed on the Device Management page.

To delete device partitions:

1. On the Junos Space Network Management Platform user interface, select **Device > Device Management.**

   The Device Management page is displayed. You can view the devices and the device partitions on this page.

2. Select the device whose device partitions you want to delete and select **Device Operations > Manage Device Partitions** from the Actions menu.

   The Manage Device Partitions page is displayed.

3. Select the device partitions that you want to delete and click the Delete Partition icon on the Actions menu.

The Delete Partition pop-up window is displayed.

4. Click **Delete**.

   The device partitions are deleted.

RELATED DOCUMENTATION

- Domains Overview | **1077**
- Creating Device Partitions | **422**
- Modifying Device Partitions | **423**

CHAPTER 21

Custom Labels

IN THIS CHAPTER

- Adding Custom Labels | 426
- Importing Custom Labels | 430
- Modifying Custom Labels | 432
- Deleting Custom Labels | 433

Adding Custom Labels

IN THIS SECTION

- Adding Custom Labels for a Device | 427
- Adding Custom Labels for Physical Inventory | 428
- Adding Custom Labels for a Physical Interface | 429
- Adding Custom Labels for a Logical Interface | 429

You add custom labels to associate user-specified data to devices, device interfaces, and device inventory. You can specify the name and the value for each custom label that you add. For example, a custom label *Location* can have a value *Building A*. Junos Space Network Management Platform provides three predefined custom labels—Device Alias, Manufacturer ID, and Manufacturer Name. The custom labels are stored in the Junos Space Platform database. You can view, modify, and delete custom labels.

NOTE: The Device Alias custom label can be added only to devices and not device interfaces or device inventory. Among the custom labels added to a device, only the Device Alias custom label can be viewed on the Device Management page. You can search, sort and filter devices on the Device Management page on the basis of the value of the Device Alias custom label.

The maximum number of characters permitted for both the custom label name and the value is 255. You cannot include any special characters except the underscore (_), the hyphen (-), and the period (.) in the name of a custom label.

Adding Custom Labels for a Device

To add custom labels for a device:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page appears, displaying the list of devices.

2. Right-click the device for which you want to add the custom label and select **Manage Customized Attributes**.

   The Manage Customized Attributes page is displayed.

3. Click the Add label icon.

   The Label Name list and the Value field are displayed. You can either choose a predefined custom label or add a custom label.

4. To choose a predefined label:
   a. Select the predefined label from the **Label Name** list.
   b. In the **Value** field, enter an appropriate value.
5. To add a custom label:
   a. In the **Label Name** list, enter a name for the label, for example, Location.
   b. In the **Value** field, enter an appropriate value for the label, for example, Building A.
6. Click **Submit**.

7. Click **Close**.

Adding Custom Labels for Physical Inventory

To add custom labels for physical inventory:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page appears, displaying the list of devices.

2. Right-click the device for which you want to add the custom label and select **Device Inventory > View Physical Inventory** from the shortcut menu.

   The **View Physical Inventory** page is displayed.

3. Right-click the physical inventory element of the device for which you want to add the custom label and select **Manage Customized Attributes**.

   The **Manage Customized Attributes** page is displayed.

4. Click the Add label icon.

   The Label Name list and the Value field are displayed. You can either choose a predefined custom label or add a custom label.

5. To choose a predefined label:

   a. Select the predefined label from the **Label Name** list.

   b. In the **Value** field, enter an appropriate value.

6. To add a custom label:

   a. In the **Label Name** list, enter a name for the label.

   b. In the **Value** field, enter an appropriate value for the label.

7. Click **Submit**.

8. Click **Close**.

Adding Custom Labels for a Physical Interface

To add custom labels for a physical interface:

1. On the Junos Space Network Management Platform UI, select **Devices > Device Management**.

   The Device Management page appears, displaying the list of devices.

2. Right-click the device for which you want to add the custom label and select **Device Inventory > View Physical Interfaces** .

   The **View Physical Interfaces** page appears, displaying the list of physical interfaces for the device.

3. Right-click the physical interface of the device for which you want to add the custom label and select **Manage Customized Attributes**.

   The **Manage Customized Attributes** page is displayed.

4. Click the Add label icon.

   The Label Name list and the Value field are displayed. You can either choose a predefined custom label or add a new custom label.

5. To choose a predefined label:

   a. Select the predefined label from the **Label Name** list.

   b. In the **Value** field, enter an appropriate value.

6. To add a custom label:

   a. In the **Label Name** list, enter a name for the label.

   b. In the **Value** field, enter an appropriate value for the label.

7. Click **Submit**.

8. Click **Close**.

Adding Custom Labels for a Logical Interface

To add custom labels for a logical interface:

1. On the Junos Space Network Management Platform UI, select **Devices > Device Management**.

   The Device Management page appears, displaying the list of devices.

2. Right-click the device for which you want to add the custom label and select **Device Inventory > View Logical Interfaces**.

The **View Logical Interfaces** page is displayed.

3. Right-click the logical interface of the device for which you want to add the custom label and select **Manage Customized Attributes** from the shortcut menu.

   The **Manage Customized Attributes** page is displayed.

4. Click the Add label icon.

   The Label Name list and the Value field are displayed.

5. In the **Label Name** list, enter a name for the label.

6. In the **Value** field, enter an appropriate value for the label.

7. Click **Submit**.

8. Click **Close**.

RELATED DOCUMENTATION

Device Management Overview | 189

Importing Custom Labels

From Junos Space Network Management Platform Release 16.1R1 onward, you can import and add custom labels to devices by using the Import Customized Attributes action on the Device Management page of the Junos Space Platform UI. Junos Space Platform enables you to add custom labels and assign values to those labels by importing CSV files containing the labels and their values.

The maximum number of characters permitted for both the custom label and the value is 255.

To import custom labels for devices by using CSV files:

1. On the Junos Space Network Management Platform UI, select **Devices > Device Management**.

   The Device Management table is displayed.

2. Select **Import Customized Attributes** from the Actions menu.

   The Import Customized Attributes Using CSV dialog box is displayed.

3. (Optional) Click the **Sample CSV** link to view a sample CSV file.

4. Click **Browse** and navigate to the location on your computer where you have stored the CSV file.

   The CSV file contains custom labels and the corresponding values for one or more devices.

5. Select the file and click **Open**.

   The name of the selected file is displayed in the CSV File text box.

6. Click **Import** to import the CSV file.

   The Job Information dialog box is displayed. You can click the job ID link or navigate to the Job Management page to view the status of the job.

7. Click **OK**.

   You are returned to the Device Management page. You can view the custom labels that you imported to a device on the Manage Customized Attributes page for that device.

   To view the custom labels added to the device, select the device on the Device Management page and select **Manage Customized Attributes** from the Actions menu. The Manage Customized Attributes page appears, displaying all the custom labels assigned to the device.

   Among the custom labels added to devices, only the Device Alias custom label and the value assigned to it can be viewed on the Device Management page.

   To view the Device Alias column, click the arrow beside any of the column names on the Device Management page, then click the arrow beside Columns to display the columns list, and select the Device Alias check box from the list.

Release History Table

Release	Description
16.1R1	From Junos Space Network Management Platform Release 16.1R1 onward, you can import and add custom labels to devices by using the Import Customized Attributes action on the Device Management page of the Junos Space Platform UI.

RELATED DOCUMENTATION

Device Management Overview | 189

Adding Custom Labels | 426

Modifying Custom Labels

You add custom labels to associate additional data to devices, device interfaces, and device inventory. You can modify or delete the custom labels associated with the devices, device interfaces, and device inventory.

To modify a custom label:

1. On the Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management table is displayed.

2. Right-click the device for which you want to modify the custom label and select **Modify Customized Attributes** from the contextual menu.

3. If you want to modify the custom label associated with a physical interface, logical interface, or the device inventory, navigate to the appropriate page.

4. Select the custom label you want to modify and change the value or the name of the label.

5. Click **Submit**.

6. Click **Close**.

RELATED DOCUMENTATION

Adding Custom Labels | 426

Deleting Custom Labels

You add custom labels to associate additional data to devices, device interfaces, and device inventory. You can modify or delete the custom labels associated with the devices, device interfaces, and device inventory.

To delete a custom label:

1. On the Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management table is displayed.

2. Right-click the device for which you want to delete the custom label and select **Modify Customized Attributes** from the contextual menu.

3. If you want to delete the custom label associated with a physical interface, logical interface, or the device inventory, navigate to the appropriate page.

4. Select the custom label you want to delete and click the Delete label icon.

5. Click **Submit**.

6. Click **Close**.

RELATED DOCUMENTATION

Adding Custom Labels | 426

CHAPTER 22

Verifying Template, Image Deployment, Script Execution, and Staged Images on Devices

IN THIS CHAPTER

- Viewing the Device-Template Association (Devices) | 434
- Viewing Associated Scripts | 437
- Viewing Script Execution | 437
- Viewing Staged Images on a Device | 438

Viewing the Device-Template Association (Devices)

You view the device-template association from the Devices workspace to determine the templates that are deployed on the device, the version of the templates deployed on the device, and find out whether the device was in sync with the template at the time the last audit was performed, as well as other relevant details.

To ensure the information presented to you is current, perform a template configuration audit immediately before viewing template association to check if there are any differences between the template configuration and the configuration on the device since the template was deployed.

To view the list of templates deployed on a device:

1. On the Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page that appears lists all the devices in the Junos Space Platform database.

2. Select the device whose template association you want to view and select **Device Configuration > View Template Association** from the Actions menu.

   The View Template Association page is displayed. This page lists the templates that are deployed to the device. The details on this page include the name of the device, IP address of the device, version of the template, time when the template was deployed to the device, Junos Space user who deployed the template, job ID for deployment, template audit status, and the time when the template was audited.

   Table 44 lists the columns on the View Template Association page.

Table 44: Viewing Template Association Page

Column Header	Description
Name	Name of the template that is deployed to the device
Domain	Domain to which the template is assigned
Deployed Version	Version of the template currently deployed to the device
Assigned Version	Version of the template currently assigned to the device
Latest Version	Latest version of the template
Deploy Time	Time at which the template was deployed to the device named in this row
Deployed By	Login ID of the person who deployed the template to the device named in this row
Job ID	ID of the job constituted by deployment of this template to the device named in this row
Audit Status	Audit status of the template: Not available, in sync or out of sync.
Audit Time	Time at which the template was deployed to the device named in this row

3. You can perform the following tasks on this page:

- To view the details of the template that is deployed to the device:

  i. Double-click on the template name.

     The Template Details pop-up window is displayed. You can view the details of the template.

  ii. Click **Close** to close the pop-up window.

- To view the configuration in the template that is deployed to the device:

  i. Click the number in the Deployed Version column.

     The Template Change Summary pop-up window is displayed. You can view the configuration that was deployed to the device.

ii. Click **Close** to close the pop-up window.

- To view the configuration in the template that is assigned to the device:

  i. Click the number in the Assigned Version column.

  The Template Change Summary pop-up window is displayed. You can view the configuration in the template that is assigned to the device.

  ii. Click **Close** to close the pop-up window.

- To view the status of the template deployment job:

  i. Click the job ID in the Job Id column.

  The Job Management page is displayed. You can view the results of the template deployment job.

  ii. Close the Job Management page.

  iii. Repeat steps 1 and 2 to navigate to the View Template Association page.

- To view the audit status of the template:

  i. Click the link in the Audit Status column.

  The Template Audit Result pop-up window is displayed.

  Under the Audit Status heading, any differences found last time the template was audited are listed. Such differences will be due to someone having altered the device configuration between the two template deployments.

  > **NOTE:** To view any differences between a template and the configuration on the devices to which it has been deployed, first ensure an audit has been performed on the template since it was deployed. For more information about auditing a template, see "Auditing a Device Template Configuration" on page 505.

4. To return to the Device Management page from the View Template Association page, click **Cancel**.

RELATED DOCUMENTATION

Deploying a Template to the Devices | 498

Viewing Associated Scripts

You can view the scripts deployed on a device to get more information about the script type, version, and activation status.

To view the scripts associated with the devices:

1. On the Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page displays the devices managed in Junos Space Network Management Platform.

2. Select the devices for which you want to view the associated scripts.

3. Select **Device Inventory** > **View Associated Scripts** from the Actions menu.

   The View Associated Scripts page is displayed.

   This page displays all the scripts that are deployed on the devices you have selected. You can view the device name, Device Alias custom label of the device, IP address of the device, platform of the device, operating system firmware version on the device, script name, script type, category of the script, staged version of the script, latest version of the script, and the activation status of the script.

Click **Back** to return to the Device Management page.

RELATED DOCUMENTATION

- Device Inventory Overview | 299
- Device Images and Scripts Overview | 609
- Executing a Script on the Devices | 358
- Viewing Script Execution | 437

Viewing Script Execution

You can view the script execution details to get more information about the scripts executed on the devices.

To view the script execution on the devices:

1. On the Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page displays the devices managed in Junos Space Network Management Platform.

2. Select the devices for which you want to view the script execution.

3. Select **Device Inventory** > **View Script Executions** from the Actions menu.

   The View Script Executions page is displayed.

   This page displays all the scripts that are executed on the devices you have selected. You can view the script name, category of the script, script version, execution status, execution results, and the start time and end time for script execution. You can also view the name and the Device Alias custom label of the device on which the script is executed.

Click **Back** to return to the Device Management page.

RELATED DOCUMENTATION

- Device Inventory Overview | 299
- Device Images and Scripts Overview | 609
- Viewing Associated Scripts | 437
- Executing a Script on the Devices | 358

Viewing Staged Images on a Device

You can view images staged on a device from the Device Management page. You can also verify the checksum from this page. Currently, you cannot view the images staged on an LSYS type device by using this workflow.

To view the images staged on a device:

1. From the Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Select the device for which you want to view the staged images and select **Device Inventory > View Staged Images** from the Actions menu.

   The View Staged Images page is displayed. Table 45 describes the columns displayed on this page.

   Table 45: View Staged Images Page

Column Name	Description
Device Name	Name of the device

Table 45: View Staged Images Page *(continued)*

Column Name	Description
Device Alias	Value of the Device Alias custom label for the device. By default, this column is not displayed on the page. The Device Alias field is empty if the Device Alias custom label is not added or no value is assigned to the Device Alias custom label of the device.
Image Name	Name of the device image
IP Address	IP address of the device
Platform	Platform to which the device belongs
Checksum Status	Whether the device image on the Junos Space server and the device are the same: • If the status is Valid, the checksum values of the device image on the Junos Space server and the device match. • If the status is Invalid, the checksum values do not match. • If the status is NA, the selected image is not staged on the device yet.
Last Checksum Time	Time when the checksum was last verified For a device on which the selected image is not staged yet, this column displays NA.

3. After you view the image staged on the device, click **Back** at the top of the View Staged Images page to return to the Device Management page.

> **NOTE:** You can select multiple devices on the Device Management page to view the images staged on these devices. Click the '+"' symbol next to the device to view the images staged on the device. The View Staged Images page lists only the devices on which the images are staged. If you select a device that does not have staged images, this device is not displayed on the View Staged Images page.

RELATED DOCUMENTATION

Device Images Overview | 613

Staging Device Images | 620

Deleting Staged Images on a Device | 457

CHAPTER 23

Device Monitoring

IN THIS CHAPTER

- Viewing Alarms from a Managed Device | 441
- Viewing the Performance Graphs of a Managed Device | 443

Viewing Alarms from a Managed Device

Starting with Junos Space Network Management Platform Release 15.2R1, you can view information about alarms from a managed device by using the Devices workspace. There are two categories of alarms: acknowledged and outstanding. You must enable the Network Monitoring functionality from the **Administration > Applications > Network Management Platform > Manage Services** page to view the list of alarms.

NOTE: You must be assigned appropriate privileges to execute this task.

To view information about the alarms from a managed device:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Devices page that appears displays all the devices managed by Junos Space Platform.

2. Right-click a device whose alarm information you need to view and select **Device Monitoring > View Alarms**.

   The View Alarms page that appears displays the list of outstanding alarms for that device, in a table.

   NOTE: The Alarms(s) outstanding search constraint is applied by default and cannot be removed. You can toggle between the Alarm(s) outstanding constraint and the Alarm(s) acknowledged constraint, which displays the list of acknowledged alarms for the selected device, by clicking the minus (–) icon.

To know more about the fields displayed in the table, see the Viewing Details of an Alarm and Acting on an Alarm section of the "Viewing and Managing Alarms" on page 844 topic.

3. (Optional) To view alarms from all Junos Space fabric nodes and managed devices, click the (–) icon corresponding to the filter in the **Search Constraints** field.

   The View Alarms page displays the list of outstanding or acknowledged alarms for all Junos Space fabric nodes and managed devices.

4. (Optional) To view a specified number of alarms per page, select the required number from the list next to the **Results** field.

   By default, the number of alarms listed on the View Alarms page is 20. You can select the number of alarms you want to view per page from the **Show** list. You can choose to view 10, 20, 50, 100, 250, 500, or 1000 alarms.

   > **NOTE:** The number of alarms selected is set as user preference and the selected number of alarms are listed beginning from the next login.

5. You can perform the following tasks on the View Alarms page:

   - Acknowledge, unacknowledge, clear, or escalate one or more alarms, or acknowledge the entire list of outstanding alarms for the selected device. For more information, see the Viewing Details of an Alarm and Acting on an Alarm section of the "Viewing and Managing Alarms" on page 844 topic.

   - Toggle between the summary and detailed views of alarms for the selected device.
     - Click the **Long Listing** link at the top of the page for a detailed view.
     - Click the **Short Listing** link at the top of the page for a summary view.

   - View the severity levels of the alarms.
     i. Click the **Severity Legend** link at the top of the page.

   For more information about summary and detailed views, and severity levels of the alarms, see the Viewing Alarms in Summary and Detailed Views section of the "Viewing and Managing Alarms" on page 844 topic.

6. Click **Back** (at the top-left corner) to return to the Device Management page.

Release History Table

Release	Description
16.1R1	To view a specified number of alarms per page, select the required number from the list next to the **Results** field.
15.2R1	Starting with Junos Space Network Management Platform Release 15.2R1, you can view information about alarms from a managed device by using the Devices workspace.

RELATED DOCUMENTATION

Alarm Notification Configuration Overview | **857**

Configuring Alarm Notification | **860**

Viewing the Performance Graphs of a Managed Device | **443**

Viewing the Performance Graphs of a Managed Device

Starting with Junos Space Network Management Platform Release 15.2R1, you can view the performance graphs of a managed device by using the Devices workspace. Performance graphs display the resources that are used on a managed device and the data collected from the managed device in a graphical format. For more information about network monitoring graphs, charts, and reports available in Junos Space Platform, refer to "Network Monitoring Reports Overview" on page 873.

NOTE: You must be assigned appropriate privileges to execute this task.

To view the performance graphs of a managed device:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Devices page that appears displays all the devices managed by Junos Space Platform.

2. Right-click a device whose performance graphs you need to view and select **Device Monitoring > View Performance Graphs**.

   The View Performance Graphs page appears. This page displays the categories of data available for the selected device. The categories include SNMP Node Data, SNMP Interface Data, Response Time, BGP Peer, OSPF Area Info, and Response Time.

3. (Optional) To select specific categories, interfaces, or resources, click **Select All** (at the bottom-left corner of the page).

4. (Optional) To clear selected categories, interfaces, or resources, click **Clear Selection** (at the bottom-left corner of the page).

   All categories, interfaces, or resources you selected are cleared.

5. To view data for all categories:

   a. Click **Graph All** (at the bottom right of the page).

      The View Performance Graphs page displays graphs for all selected categories. By default, the graphs display the data from the previous day.

   b. (Optional) To change the period of time, select the appropriate time period from the Time Period field at the top of the page.

      The options available are Last day, Last week, Last month, Last Year, and Custom.

      If you select Custom:

      i. Enter the start time (month, date, year, and time) in the Start Time field.

      ii. Enter the end time (month, date, year, and time) in the End Time field.

      iii. Click **Apply Custom Time Period**.

         The data is refreshed to reflect the time period specified.

6. To view data for a specific category or interface:

   a. Select the check box corresponding to the category or interface.

   b. Click **Graph Selection** (at the bottom of the page).

      The View Performance Graphs page displays graphs for the selected category or interface. By default, the graphs display the data from the previous day.

   c. (Optional) To change the period of time, select the appropriate time period from the Time Period field at the top of the page.

      The options available are Last day, Last week, Last month, Last Year, and Custom.

      If you select Custom:

      i. Enter the start time (month, date, year, and time) in the Start Time field.

ii. Enter the end time (month, date, year, and time) in the End Time field.

iii. Click **Apply Custom Time Period**.

The data is refreshed to reflect the time period specified.

7. To search and view data for specific resources (categories or interfaces):

a. Click **Search** (at the bottom right of the page).

The Search for Node field is displayed.

b. Enter a text string to identify the resources of the device that you want to view and click **OK**.

The View Performance Graphs page that appears displays the filtered view.

c. Select the check box corresponding to the category or interface.

d. Click **Graph Selection** (at the bottom of the page).

The View Performance Graphs page displays graphs for the selected category or interface. By default, the graphs display the data from the previous day.

8. Click **Back** (at the top-left of the page) to return to the Device Management page.

Release History Table

Release	Description
15.2R1	Starting with Junos Space Network Management Platform Release 15.2R1, you can view the performance graphs of a managed device by using the Devices workspace.

RELATED DOCUMENTATION

Alarm Notification Configuration Overview | 857

Configuring Alarm Notification | 860

Viewing Alarms from a Managed Device | 441

CHAPTER 24

Device Maintenance

IN THIS CHAPTER

- Viewing Device Statistics | 446
- Viewing Devices and Logical Systems with QuickView | 447
- Resynchronizing Managed Devices with the Network | 448
- Putting a Device in RMA State and Reactivating Its Replacement | 449
- Modifying the Target IP Address of a Device | 453
- Modifying the Serial Number of a Device | 455
- Rebooting Devices | 456
- Deleting Staged Images on a Device | 457
- Cloning a Device in Junos Space Network Management Platform | 458
- Deleting Devices | 459

Viewing Device Statistics

You can view device statistics when you select the Devices workspace. The charts presented on the Devices page display the connection status of the devices, number of devices per OS, number of devices per platform, and the auto-resynchronization state of the devices. All the charts are interactive.

The Devices page displays the following charts:

- Device Count by Platform—Number of Juniper Networks devices organized by type
- Device Status—Number of devices organized by the connection status on the network
- Device Count by OS—Number of devices running a particular Junos OS release
- Device Count by Synchronization State—Number of devices organized by auto-resynchronization state

To view device statistics:

1. On the Junos Space Network Management Platform user interface, select **Devices**.

   The Devices page is displayed. This page displays the charts related to the devices.

2. Click a specific label on a chart.

   You are redirected to the Device Management page, the contents of which are filtered based on the label you clicked.

   To save the chart as an image or to print the chart, right-click the chart and select Save or Print respectively.

RELATED DOCUMENTATION

- Viewing Managed Devices | 194
- Viewing the Physical Inventory | 301
- Device Discovery Profiles Overview | 220

Viewing Devices and Logical Systems with QuickView

The QuickView feature shows you the type and status of a device or logical system using an icon.

To view a device or logical system using Quick View:

1. On the Network Management Platform user interface, select **Devices > Device Management**.

2. Select the Quick View action button on the menu bar.

3. Alternatively, at the right edge of the Network Management Platform page, find the sidebar open arrow for the Device Management table.

   NOTE: Be careful to find the correct sidebar open arrow. There are two; one on the left that opens the Quick View sidebar, and one on the right that opens the Help panel.

   The Quick View sidebar arrow in green. The other arrow, highlighted in red, opens the Help sidebar.

4. Click the Quick View sidebar open arrow.

   Platform opens the Quick View sidebar. The Quick View shows the status of the device that is currently selected in the table.

You can close the Quick View window in the same way that you opened it.

RELATED DOCUMENTATION

- Understanding Logical Systems for SRX Series Services Gateways | 417
- Viewing the Physical Device for a Logical System | 420
- Viewing Logical Systems for a Physical Device | 420
- Creating a Logical System (LSYS) | 418
- Deleting Logical Systems | 419

Junos OS Logical Systems Configuration Guide for Security Devices

Resynchronizing Managed Devices with the Network

If the network is the system of record, you can resynchronize a managed device at any time. For example, when a managed device is updated by a device administrator from the device's native GUI or CLI, you can resynchronize the device configuration in the Junos Space Network Management Platform database with the physical device. (If Junos Space Network Management Platform is the system of record, this capability is not available. See "Systems of Record in Junos Space Overview" on page 214.)

To resynchronize a device:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page appears.

2. Select the devices you want to resychronize and select **Device Operations > Resynchronize with Network** from the Actions menu.

   The Resynchronize Devices pop-up window is displayed.

3. Click **Confirm**.

   When a resynchronization job is scheduled to run but another resynchronization job on the same device is in progress, Junos Space Network Management Platform delays the scheduled resynchronization job. The time delay is determined by the damper interval that you set from the application workspace. By default the time delay is 20 seconds. The scheduled job is delayed as long as the other resynchronization job to the same device is in progress. When the job that is currently running finishes, the scheduled resynchronization job starts. See "Modifying Settings of Junos Space Applications" on page 1345.

NOTE: You can check whether a managed device was resynchronized with the network, from the Job Details page. To go to the Job Details page, double-click the ID of the resynchronization job on the Job Management page. The Description column on this page specifies whether the managed device was resynchronized with the network. If the managed device was not resynchronized with the network, the column lists the reason for failure. If there is an error, the View Job Details page displays an error message. For more information about the error messages, see "Common Error Messages in Device-Related Operations" on page 992.

RELATED DOCUMENTATION

Understanding How Junos Space Automatically Resynchronizes Managed Devices | 216

Systems of Record in Junos Space Overview | 214

Device Inventory Overview | 299

Viewing the Physical Inventory | 301

Viewing Physical Interfaces of Devices | 306

Exporting the License Inventory | 312

Putting a Device in RMA State and Reactivating Its Replacement

IN THIS SECTION

Putting a Device in RMA State | 450

Reactivating a Replacement Device | 451

Sometimes, because of hardware failure, a device managed by Junos Space Network Management Platform needs to be returned to the vendor for repair or replacement. In such cases, Junos Space Network Management Platform can keep on record the configuration of the defective device until you can obtain an equivalent replacement device from the vendor. You create this record by putting the defective device in Return Materials Authorization (RMA) state before removing it. In this way, you prevent the configuration from being deleted from the Junos Space Network Management Platform database when the device is removed.

Before connecting the replacement device, you must configure it with such basic information as the name, IP address, SSH fingerprint, and login credentials.

After the replacement device has been reconnected within your network, you perform the Reactivate from RMA task to cause Junos Space Network Management Platform to read its settings, deploy the preserved configuration onto it, and bring it back under management. Because the two devices are perceived as equivalent, this operation is considered *re*activation, even if the replacement device is new.

Do not delete or physically disconnect the defective device before performing the Put in RMA State task.

WARNING: Remove any provisioning services associated with a device before putting it in RMA state.

Putting a Device in RMA State

If you want to return a device to the vendor under RMA, but you do not want to delete its configuration from the Junos Space Network Management Platform database, put the device in RMA state.

To have Junos Space Network Management Platform keep on record the configuration of a defective device so that you can later deploy that configuration to the defective device's replacement:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Select the defective device and select **Device Operations > Put in RMA State** from the Actions menu.

   The RMA Device window appears.

3. Click **Confirm** to put the selected device in RMA state.

SEE ALSO

Viewing Managed Devices | 194

Deleting Devices

Resynchronizing Managed Devices with the Network | 448

Reactivating a Replacement Device

Before you begin, you must perform basic configuration on the replacement device, such as the name, IP address, SSH fingerprint, and login credentials. TheIP address must match that of the original device when it was put in RMA state.

From Junos Space Network Management Platform Release 18.2 onward, you can reactivate multiple replacement devices at the same time. The maximum number of devices that can be reactivated simultaneously is 100.

To reactivate the replacement device:

1. Connect the replacement device to your network in the same way as the defective device was connected.

2. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

3. Select the items that formerly represented the defective devices. (It in fact now represents the replacement device, without the need for you to make any changes to it.)

4. Select **Device Operations > Reactivate from RMA** from the Actions menu.

   The Reactivate Device from RMA page is displayed listing the selected items representing the replacement devices. The device name and IP address of the device is displayed for each item on this list.

   By default, the New fingerprint column will be empty for every device. User can manually enter the new device fingerprint or leave it empty.

5. Enter the new fingerprint manually or import fingerprints in the form of a CSV file.

   To import SSH fingerprint using a CSV files:

   - Click **Browse** and select the CSV file to be uploaded from your local file system.

   - Click **Upload** to upload the selected CSV file.

     Once the file is uploaded, the details of the devices to be reactivated - device name, IP address of the device, and new SSH fingerprint is displayed in the grid.

   - (Optional) To download a sample CSV file, click the **Sample CSV** link.

A sample CSV file listing the name, IP address, and new SSH fingerprint of the devices to be reactivated.

6. (Optional) If there is no SSH fingerprint displayed for an device or if you want to associate a new SSH fingerprint with the reactivated device, a fingerprint conflict occurs.

   To auto-resolve SSH fingerprint conflicts, select the **Auto-resolve fingerprint conflict if new fingerprint is not provided** check box. If you choose select this check box, the fingerprint conflict resolution settings saved in the Device section of Modify Application Settings page (Administration > Applications) is overridden for device reactivation from RMA.

7. To push the existing device configuration from Junos Space:

   - (Optional) Select the **Push existing device configuration from Junos Space** check box to push the configuration saved in Junos Space to the reactivated device.

     NOTE: If you choose to push existing device configuration from Junos Space, scripts that were staged on the replaced device is restaged to the reactivated devices.

     If you choose not to push existing device configuration from Junos Space, all the scripts associated with the device is removed.

   - To use commit -confirmed for the reactivated devices, select the **Use commit -confirmed** check box.

   - To use temporary credentials to push device configuration from Junos Space, select the **Use temporary device credentials to push configuration** check box.

     Enter the temporary username and password to push the configuration.

     NOTE: The temporary username and password will be used only to push the existing configuration from Junos Space on to the reactivated devices.

8. Click **Confirm** to activate the replacement devices.

   The Reactivate Devices from RMA Job page appears displaying the job Id for the reactivation job. To view details of the job, click on the job ID.

   The replacement devices are displayed with the defective devices' configuration in the Device Management page. As activation proceeds, intermediate states such as Reactivating are displayed under

Managed Status. The replacement devices are active and under management when Connection Status reports that the device is up, and Managed Status reports In Sync.

If Junos Space Platform detects an SSH fingerprint mismatch between that on the device and the fingerprint stored in the Junos Space Platform database, the connection is dropped. The connection status is displayed as Down and the authentication status is displayed as Fingerprint Conflict on the Device Management page.

SEE ALSO

Viewing Managed Devices | 194

Deleting Devices

Resynchronizing Managed Devices with the Network | 448

Modifying the Target IP Address of a Device

You modify the target IP address of a device when you need to change the IP address that Junos Space Network Management Platform will use to connect to the device. When you modify the IP address, the device connects to Junos Space Platform with the new IP address. You can use this workflow to migrate from IPv4 to IPv6 and from IPv6 to IPv4 addresses. You cannot use this workflow to modify the target IP address of a ww Junos OS device.

The IP address modified using this workflow is only stored in the Junos Space Platform database. The modified IP address is not configured on the device. You need to either modify the device configuration and update the new IP address manually or push this IP address configuration to the device by using the Device Templates feature.

NOTE: This workflow is supported only for Junos Space-initiated connections.

To modify the target IP address of a device in Junos Space Platform:

1. On the Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page that appears displays the list of devices managed on Junos Space Platform.

2. Right-click the device you need to modify and select **Device Access > Modify Device Target IP**.

   The Modify Device Target IP page is displayed.

3. Click the New IP column on the page.

   An inline editor is displayed.

4. Enter the target IP address of the device.

   NOTE: You can enter the IP address in either IPv4 or IPv6 addressing formats.

5. Click **Modify**.

   The new target IP address for the device is displayed on the Device Management page.

When you complete this workflow, Junos Space Platform performs the following steps to ensure that the device is reachable with the new IP address:

a. Establishes an SSH connection to connect to the device on the new IP address and obtains the serial number of the device

b. Verifies the serial number of the device against the serial number stored in the Junos Space Platform database. If the serial number returned from the device matches the one in the Junos Space Platform database, the new IP address is updated in the Junos Space Platform database. If the serial number verification fails, the job triggered for this workflow fails.

c. Resets the connection to the device and waits for the device to connect back to Junos Space Platform in about five minutes. If the device does not connect to Junos Space Platform in about five minutes, the job triggered for this workflow fails.

NOTE: If the job triggered for this workflow fails, Junos Space Platform does not revert the IP address to the one stored in the Junos Space Platform database.

RELATED DOCUMENTATION

Device Management Overview | 189

Viewing Managed Devices | 194

Junos Space IPv6 Support Overview | 1152

Modifying the Serial Number of a Device

You modify the serial number of a device that is added to Junos Space Network Management Platform.

To modify the serial number of a modeled device:

1. On the Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Select the modeled device for which you want to modify the serial number and select **Device Operations > Modify Serial Number** from the Actions menu.

   The Modify Serial Number page is displayed.

3. Double-click the serial number in the Serial Number column of the device and enter the new serial number.

4. Click **Modify**.

   The serial number of the modeled device is modified.

RELATED DOCUMENTATION

- Model Devices Overview | 251
- Creating a Modeled Instance | 257
- Adding More Devices to an Existing Modeled Instance | 274
- Downloading a Configlet | 266
- Viewing and Copying Configlet Data | 268

Rebooting Devices

You can reboot devices from Junos Space Network Management Platform. You can also reboot virtual chassis setups, dual Routing Engine (RE) setups, and cluster setups from Junos Space Network Management Platform. You cannot reboot Logical System (LSYS) devices from Junos Space Network Management Platform.

To reboot devices:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Select the devices that you want to reboot and select **Device Operations > Reboot Devices** from the Actions menu.

   The Reboot Devices pop-up window is displayed. This pop-up window displays the devices that you selected for reboot and some additional options that you can configure before the reboot.

3. (Optional) Select the **Options** option button. Configure the following options in this section:

   a. In the **Message** field, enter a message to indicate the purpose of this reboot operation.

   b. Select the **Power off** option button.

4. (Optional) To schedule a time for reboot, select the **Schedule at a later time** option button and use the lists to specify the date and time.

5. Click **Confirm**.

   The devices that you selected will be rebooted. A job will be created. You can view the job results from the Job Management page. If some of the devices fail to reboot, you can use the Retry on Failed Devices action to retry rebooting the devices that failed to reboot. For more information, see "Retrying a Job on Failed Devices" on page 980. When you reboot devices, an audit log entry is automatically generated. You can view the audit logs from the Audit Logs workspace.

> **NOTE:** To reboot a single device, select only one device on the Device Management page and select **Device Operations > Reboot Devices** from the Actions menu.

RELATED DOCUMENTATION

Device Management Overview | 189
Viewing Managed Devices | 194

Deleting Staged Images on a Device

You can delete images staged on a device from the Device Management page. Currently, you cannot delete the images staged on an LSYS type device by using this workflow..

To delete the images staged on a device:

1. From the Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Select the device from which you want to delete the staged images and select **Device Inventory > View Staged Images** from the Actions menu.

   The View Staged Images page is displayed.

3. Select the staged images that you want to delete from the device.

4. Click the Delete Images icon on the Actions menu.

   A job is created. You can view the status of the job on the Job Management page.

5. After you delete the staged images on a device, click **Back** at the top of the View Staged Devices page to return to the Device Management page.

> **NOTE:** You can select multiple devices on the Device Management page to delete the images staged on these devices. Click the “+” symbol next to the each device, select the staged images, and click the Delete Images icon on the Actions menu. The View Staged Images page lists only the devices on which the images are staged. If you select a device that does not have staged images, this device is not displayed on the View Staged Images page.

RELATED DOCUMENTATION

Device Images Overview | 613
Staging Device Images | 620

Viewing Staged Images on a Device | 438

Cloning a Device in Junos Space Network Management Platform

You clone devices to create copies of managed and modeled devices in Junos Space Network Management Platform. You can clone modeled devices even if they are in the Modeled or Waiting for Deployment state. You cannot clone unmanaged devices in Junos Space Platform. The cloned copy of the device is displayed by default as being in the Modeled state on the Device Management page.

> **NOTE:** You need to activate a cloned device by using the Activate workflow to manage the device in Junos Space Platform.

To clone a device in Junos Space Platform:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page that appears displays the list of devices that exist in the Junos Space Platform database.

2. Select the device to clone and select **Device Operations > Clone Device** from the Actions menu.

   The Clone Device page is displayed. The device family and platform of the device are displayed on this page.

3. In the **Clone Device Name** field, enter the name of the device.

   The name of the cloned device should start and end with letters or numbers and cannot exceed 255 characters. The hyphen (-) and underscore (_) are the only special characters allowed. Leading and trailing spaces are not allowed.

4. In the **Number of Devices** field, use the up and down arrows to specify the number of devices to be cloned using this workflow.

   The default value is 1.

5. (Optional) Select the **Image Upgrade/Downgrade** check box to upgrade or downgrade the cloned device to a specific Junos OS version.

6. (Optional) From the **Device Image** drop-down list, select the device image that contains the Junos OS version to which you want to upgrade or downgrade the devices.

7. Click **Clone**.

   You are redirected to the Device Management page. When the device is cloned, the device is added to the Device Management page. The managed status of this device is set to Modeled.

> **NOTE:** Devices created using this workflow are given the original name of the device appended with "_#" where # is a number. The devices are numbered from 1 through the value you specified for the number of devices. For example, if you clone a device named "device" and create three devices, they are named "device_1," "device_2," and "device_3."

RELATED DOCUMENTATION

- Model Devices Overview | **251**
- Viewing Managed Devices | **194**
- Activating a Modeled or Cloned Device in Junos Space Network Management Platform | **262**

Deleting Devices

You can delete devices from Junos Space Network Management Platform. Deleting a device removes all device configuration and device inventory information from the Junos Space Network Management Platform database.

If provisioning services are associated with a device that you want to delete, you must remove the provisioning services before deleting the device.

To delete devices:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page appears.

2. Select the devices you want to delete and select **Device Operations > Delete Devices** from the Actions menu.

   The Delete Devices pop-up window is displayed.

3. Click **Confirm.** .

   Junos Space Network Management Platform deletes all device configuration and inventory information for the selected devices from the Junos Space Network Management Platform database.

RELATED DOCUMENTATION

- Viewing Managed Devices | **194**
- Viewing the Physical Inventory | **301**
- Viewing Physical Interfaces of Devices | **306**
- Device Discovery Profiles Overview | **220**

3

PART

Device Templates

Overview | **462**

Template Definitions | **471**

Configuring Devices using Device Templates | **494**

Configuring Devices using Quick Templates | **508**

Device Template Administration | **520**

CHAPTER 25

Overview

IN THIS CHAPTER

- Device Templates Overview | 462

Device Templates Overview

IN THIS SECTION

- Template Definition | 464
- Device Template States | 467
- Device Template Statuses | 467
- Device Templates Workflow | 467
- Device Template Deployment | 469

The Device Templates workspace in Junos Space Network Management Platform provides the tools to create custom device templates and deploy common configuration to multiple devices from the Junos Space user interface. Device templates are schema-driven, so you can access and configure all the configuration parameters for any device supported on Junos Space Platform. For example, with device templates, you can create the build of a new device. You can configure routing protocols, such as BGP, OSPF, IS-IS, and static routes.

You can create two types of device templates in Junos Space Platform:

- *Configuration template* – A configuration template is a template created by using a template definition. You first create a template definition and specify the common configuration that can be deployed to a device. You then create a device template by using the template definition, assign values to the common configuration parameters, and deploy the template to the device.
- *Quick template* – A Quick template is a template created without using a template definition. For more information about Quick templates, see "Quick Templates Overview" on page 508.

The Templates page in the Device Templates workspace lists the device templates created in tabular view. Table 46 lists and describes the columns of the table.

Table 46: Templates Page

Column Name	Description
Name	Name of the device template
Domain	Domain to which the device template is assigned
Template Type	Type of the device template: Quick Template or Config Template
Latest Version	Latest version of the device template
Description	Description of the device template
Last Modified By	Login name of the operator who last modified the device template
Last Update Time	Time when the device template was last updated
State	Deployment readiness of the device template: Needs Review, Disabled, or Enabled
Deployment Status	Deployment status of the template: Created, Assigned, or Deployed

Template definitions are usually created by the Template Design Manager user role. Definition-based templates and Quick templates are created by the Template Manager user role. The following sections describe a template definition, device template, and the workflow to create and deploy templates:

Template Definition

A template definition is the building block of the configuration you create by using the device template feature. A template definition restricts the scope of the device template to a specific device family and Junos OS version.

When you create a template definition, you define the following aspects of the configuration options in the template definition:

- Custom validation rules and error messages. For more information, see "Working with Rules in a Template Definition" on page 480.
- Default values or device-specific values. You can also set up CSV files (outside of Junos Space Platform) as a basis for your template definitions. For more information, see "Specifying Device-Specific Values in Template Definitions" on page 482. CSV file values take precedence in case of conflicts with rules-based values.
- Whether the configuration option is editable, read-only, or hidden

The data type of a configuration option is predefined in the DMI schema . You can modify the data type of the configuration option when you create the template definition. The data type of a configuration option determines the configurability of the option in the final definition. You can organize these configuration options across multiple pages.

Table 47 lists the data types for the configuration options and the tabs associated with each type. An * (asterisk) indicates that the tab is available for the corresponding data type. An — (en dash) indicates that the tab is not available for the corresponding data type. The DMI schema determines the data type, method of validation, and how the parameters are displayed.

To create a useful template definition, the Template Design Manager must determine in advance which parameters or configuration options he or she wants the Template Manager to set, which parameters are to be read-only, and which parameters, if any, are to be hidden from the Template Manager. The data type of an option determines how the data will be displayed and what tabs are available to enter data.

Table 47: Data Types and Tabs

		Tabs			
Data Types	Description	**General**	**Description**	**Validation**	**Advanced**
Container	The Container data type holds other data types.	*	*	—	—
Table	The Table data type displays a list of records with identical structures.	*	*	*	*

Table 47: Data Types and Tabs *(continued)*

Data Types	Description	Tabs			
		General	**Description**	**Validation**	**Advanced**
String - Key column in a table	The String - Key column in a Table data type identifies the uniqueness of the record in the table. If the table has a key specified, only one record with the given key can exist.	*	*	*	*
String	The String data type contains character strings.	*	*	*	*
Integer [Number]	The Integer [Number] data type is used to specify a numeric value without a fractional component.	*	*	*	*
Boolean	The Boolean data type has two possible values: true and false. The value is True if selected and False if not selected.	*	*	—	*
Enumeration	The Enumeration data type defines a variable to be a set of predefined constants. The variable must be equal to one of the values that has been predefined for it. Use this data type to create drop-down lists.	*	*	—	*
Choice	The Choice data type provides an option button. Select the option button to use the configuration option in the template.	*	*	—	*

Table 48 lists the validation parameters for the data types that require validation.

Table 48: Data Types and Validation Parameters

Data Type	Validation Parameters		
Integer [Number]	Min Value	Max Value	
String	Min Length	Max Length	Regular Expression
Table	Min Occurrence	Max Occurrence	
String - Key column in a table	Min Length	Max Length	Regular Expression

All configuration options of the Table data type have a key column by default.

The Definitions page in the Device Templates workspace lists the template definitions in tabular view. Table 49 lists and describes the columns of the table.

Table 49: Definitions Page

Column Name	Description
Name	Name of the template definition
Domain	Domain to which the template definition is assigned
Description	Description of the template definition
Device Family	Juniper Networks DMI Schema; for example, J Series, M Series, MX Series, T Series, and TX Series
Last Modified By	Login name of the template designer who last modified the template definition
Last Update Time	Time when the template definition was last updated
State	State of the template definition: published or unpublished

Junos Space Network Management Platform assigns different states to the template definitions. These states are listed in the State column of the table on the Definitions page. When a Template Design Manager finishes creating a template definition, that definition is automatically published by default. Template Design Managers can perform a series of operations on the definitions, but to do so, they must first unpublish the definitions. The Template Manager can see only published definitions; they cannot see unpublished definitions.

The Template Design Manager specifies not only which device parameters appear in the definition, but also which parameters can be edited by the Template Manager when he or she creates a template. The Template Design Manager also sets the defaults for the editable parameters.

NOTE: You cannot edit, publish, or delete a template definition if the template definition is being edited by another user. You receive a pop-up message indicating the user who is currently editing the template definition.

Device Template States

Junos Space Platform assigns different states to the device templates based on their deployment readiness. Table 50 lists the states and their descriptions.

Table 50: Device Template States

State	Description
Needs Review	The device template cannot be deployed until you review it. This state is triggered by a designer who is modifying the template definition on which the device template is based. That device template is then automatically moved to the Needs Review state.
Disabled	The device template cannot be deployed. This state is triggered by the designer unpublishing the template definition upon which a device template is based. That device template is then automatically disabled.
Enabled	The device template can be deployed. As soon as you finish creating a device template, it is enabled automatically.

Device Template Statuses

Junos Space Platform assigns different deployment statuses to the device templates. Table 51 lists the deployment statuses and their descriptions.

Table 51: Device Template Deployment Statuses

Deployment Status	Description
Created	The device template displays this status if: • The device template is not yet assigned or deployed to the device. • The device template is undeployed or unassigned from the device.
Assigned	The device template is assigned to the device.
Deployed	The device template is deployed to the device.

Device Templates Workflow

Device templates can be designed to allow (or prevent) specified tasks to be (or from being) performed by two predefined Junos Space Platform user roles:

- Template Design Manager—A designer who understands both:
  - The technical details of the device configuration

  - How to implement this knowledge to solve specific business problems
- Template Manager—An operator who executes the instructions of the Template Design Manager

A Template Design Manager (hereafter referred to as “designer”) creates template definitions and publishes them. A Template Manager (hereafter referred to as “operator”) selects a template definition and creates the device template from the template definition to configure one or more devices. The operator then tests the device template on the device (without deploying it). If the device template is validated, the operator deploys the device template to the device. With this division of labor, the operator does not need specialist knowledge. Alternatively, if one person is assigned both roles, using device templates radically reduces the volume of work and virtually eliminates operator error.

While creating the definition, the designer can verify what the operator sees when creating a device template from the definition. The operator, however, can gain no insight into what the designer saw when creating the definition. This has important consequences: while the designer can identify configuration options simply through their place in the hierarchy represented as a tree, the operator is entirely dependent on the label of the option. It is by means of the label alone that an operator determines which parameter he or she is configuring.

Designers can choose not only which options to display to the operators, but also whether to display them at all. They can make configuration options editable or read-only, and even provide customized explanations for the operators. Operators can immediately deploy a device template to the devices they select or schedule deployment for a later date.

Ensure that the following requirements are met to use the device template workflows successfully:

- To be available for use by operators, template definitions must be published. Template definitions that are unpublished are not available for the creation of templates.
- Templates based on a definition that was unpublished after the templates were created are automatically disabled.
- Templates based on a definition that was unpublished and then republished are marked as needing review. They cannot be deployed before an operator reviews them.
- Templates based on a definition that has been deleted are permanently disabled.
- Templates based on a published definition that has not been unpublished in the meantime are enabled.

NOTE: You cannot edit or delete a device template if the device template is being edited by another user. You receive a pop-up message indicating the user who is currently editing the device template.

NOTE: We recommend that you do not navigate to other pages or other Junos Space applications when modifying a device template or a template definition. Save the changes before you navigate to other pages or other Junos Space applications.

Device Template Deployment

You can add and delete configuration details to and from device templates before deploying the template to a device. You can assign, deploy, unassign, and undeploy device templates to and from IPv4-enabled and IPv6-enabled devices manually, by using tags, or by using a CSV file. Assigning a device template to a device allows you to view the consolidated configuration changes to be deployed on the device from the Devices workspace. You can choose to include or exclude the configuration changes in or from the device template when you deploy the consolidated configuration changes by using the Review/Deploy Configuration workflow from the Devices workspace. For more information, see "Reviewing and Deploying the Device Configuration" on page 327. A device template that has been assigned to a device cannot be deployed using the Deploy workflow.

When you deploy a device template to a device, the unconfigured parameters are also committed. This means that if you applied two device templates to a device, only the configuration contained in the last device template is retained. For example, if you set the SNMP location in the first device template that you deployed, but did not do so in the second device template, the SNMP location information is lost as soon as you deploy the second device template. Therefore, to build a complex configuration by applying multiple device templates in stages, you should modify the last deployed definition or device template each time you add a layer of complexity.

With Junos Space Network Management Platform as the System of Record (in SSOR mode), you can deploy a template on a device in two ways:

- Assign a template to a device by using the **Assign to Device** workflow in the Device Templates workspace, and approve and deploy the template by using the **Review/Deploy Configuration** workflow in the Devices workspace.
- Deploy a template to a device by using the **Deploy** workflow in the Device Templates workspace.

If you assign a template to a device and use the Deploy workflow to deploy that template on the same device, although the template is deployed to the device, Junos Space Platform does not reflect this managed status. The managed status of the device is shown as "Space Changed" on the Device Management page.

RELATED DOCUMENTATION

Creating a Template Definition | 471

Finding Configuration Options in a Template Definition | 478

Working with Rules in a Template Definition | 480

Creating a Device Template | 494

CHAPTER 26

Template Definitions

IN THIS CHAPTER

- Creating a Template Definition | 471
- Finding Configuration Options in a Template Definition | 478
- Working with Rules in a Template Definition | 480
- Specifying Device-Specific Values in Template Definitions | 482
- Managing CSV Files for a Template Definition | 485
- Publishing a Template Definition | 486
- Viewing a Template Definition | 486
- Modifying a Template Definition | 488
- Cloning a Template Definition | 489
- Importing a Template Definition | 490
- Exporting a Template Definition | 491
- Unpublishing a Template Definition | 492
- Deleting a Template Definition | 493

Creating a Template Definition

You create a template definition to create custom device templates that can be deployed to devices through Junos Space Network Management Platform.

To create a template definition:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

   The Definitions page is displayed.

2. Click the **Create Template Definition** icon on the Actions menu.

   The Create Template Definition page is displayed.

3. From the Device Family Series section, select the device family to which your template definition will apply.

   The Junos OS versions and hardware platforms supported by the selected device family appear in the Description section on the right. The OS version that appears on the drop-down list in the OS Version section below the Device Family Series section is the one that is set as default for that device family.

   > **NOTE:** It is recommended to include the device family and OS version information in the description of the template definition. Unless you include the information in the definition name or description, the operator will not know which device family this definition applies to.

4. Select the appropriate OS version from the drop-down list in the OS Version section below the Device Family Series section.

   > **NOTE:** If you do not use the latest DMI schema , you will not have access to the most recent device configuration options.

5. Click **Next**.

6. In the **Name** field, type a user-defined template definition name.

   A template definition name cannot exceed 128 characters and can contain only letters, numbers, spaces, and some special characters. The special characters allowed are hyphen (-), underscore (_), period (.), at (@), single quotation mark ('), forward slash (/), and ampersand (&).

7. (Optional) In the **Description** field, type a user-defined description.

   The description cannot exceed 256 characters. The operators who use the template definition to create templates rely on the description for information about the template definition.

8. From the Available Configuration section on the left, select one of the following from the drop-down list:

   - View All Configuration — Provides all configuration options available for the selected device family's default DMI schema
   - Common Configuration — Provides the parameters typically configured for the selected device family—for example, for J Series, M Series, MX Series, TSeries, and TX Series devices, the parameters are Interfaces, Routing options, SNMP, and System.

- MPLS Pre-staging — Provides the parameters necessary to configure MPLS for the selected device family—for example, for J Series, M Series, MX Series, T Series, and TX Series devices, the parameters are Interfaces, Protocols, and Routing options.

9. Display the hierarchy of Junos OS configuration options available for the device family by clicking the plus sign to the left of the Configuration node at the top of the tree.

   The hierarchy appears in the form of a tree. Each item can be expanded by clicking the plus sign.

10. (Optional) Click the configuration option that you want to configure for this template definition. To find configuration options, see "Finding Configuration Options in a Template Definition" on page 478.

    The Selected Configuration Layout section on the right of the page displays the configuration pages. A default page, Config Page 1, is available to hold your groups of configuration options. You can create additional pages by clicking the Add Configuration Page icon at the top of the Selected Configuration Layout section.

11. (Optional) To rename the configuration page and enter a description:

    a. Select the configuration page in the left panel of the Selected Configuration Layout section.

    b. In the **Label** field, enter a user-defined configuration page name.

    c. In the **Description** field, enter a user-defined description.

    > **NOTE:** Delete a page by selecting a page from the left panel of the Selected Configuration Layout section and clicking the Delete Selected Page or Option icon.

12. To choose the configurable options, drill down through the hierarchy in the Available Configuration section. Unless you have opened a directory, selecting it and moving it does not transfer the directory's contents into your template definition. You can select multiple options simultaneously by holding down the Ctrl key.

    You can move an option from the Available Configurations panel to a page in the Selected Configuration Layout panel in three ways:

    - Drag one or more options from the Available Configuration panel to the Selected Configuration Layout panel, and drop it directly onto the appropriate page in the Selected Configuration Layout panel.
    - First, select the destination page in the Selected Configuration Layout panel, then select the options to be moved.

      Click the orange arrow between the panels.

      The option moves from the Available Configuration panel to the Selected Configuration Layout panel.

- First, select a page in the Selected Configuration Layout panel, then double-click an option in the Available Configuration panel.

  The option moves to the selected page. Note that the page does not open automatically. The minus sign to the left of an empty page changes to a plus sign if the move was successful.

Any sequence is permissible, and there is no limit on the number of options a page can hold. You cannot put children of the same parent into different pages. If you drill down and select a parameter deep in the hierarchy, dragging that parameter causes all the other parameters that require configuration to come with it.

You can create field labels on the General tab to help the operator enter correct field data. The General tab applies to both the configuration pages and the configuration options you select.

13. To create a field label for configuration options, in the Selected Configuration Layout section, select a configuration option.

    The General tab displays the default text.

14. (Optional) To rename the selected option, in the **Label** field, overwrite the default or existing name.

    > **TIP:** Because the configuration options lose their context when you move them out of the tree in the Available Configuration section, consider changing the default labels to indicate to operators creating device templates what these parameters are for. The default labels are ambiguous without the context of the tree. For example, there are many options called *pool*.

    The Data Type box displays the selected option's data type, which determines not only the tabs displayed, but also the method of validation.

15. (Optional) If the data type of an option is String, it is possible to provide the template administrator or operator a drop-down list to choose from when creating templates from this definition. To provide a drop-down list of choices, change the data type of the selected option to Enumeration by clicking the **Enumeration** option button in the Data Type box.

    Either a box containing ready-made choices appears, or a box to contain the choices you create appears, and next to it, a green plus [+] and a red minus [–] icon.

    - To create each drop-down list choice, click the green plus [+] icon

      A text field appears, to the right of which is an OK button, a Close button, and a red X.

    - Enter text in the field (limit 255 alphanumeric characters) and click **OK** when finished.

      The newly created choice appears in the box to the left of the text field.

> **TIP:** Keep your choices short;, otherwise, they are hard to read when you specify the default values or when the operator tries to select them from the list. You can create up to 23 choices.

- (Optional) To delete a drop-down list choice, select the choice and click the red minus [–] icon.

  The choice disappears from the box.

- To finish adding choices, click **Close** or the red X to the right of the text field.

16. To save your entries on the General tab, select another tab or another option, or click **Next**.

    You can add descriptive text in the Description tab. This can help the operator enter the correct data. When the operator creates a device template, he or she can view your description or explanation by clicking the little Information icon to the right of the parameter (in the template). A pop-up box appears, displaying the content you entered in the Description field.

17. To change the default description, click the **Description** tab.

18. In the **Description** field, enter a user-defined description for the selected configuration option.

19. To save your the description, move to another tab or another option, or click **Next**.

    The Validation tab displays the validation criteria for the selected configuration option. Not all options have Validation tabs. The validation criteria are determined by the option's data type: string, integer/number, table, container, choice, or enumeration. When you define fields in which you intend the operator to enter content, you usually restrict or limit that content in order to prevent validation errors during deployment. For example, if you define a field that you label **Hostname**, you could use a regular expression to prevent the operator from entering anything other than an IP address. Another situation might be when a particular attribute allows values A, B, C, D, or E, but you want templates that allow only values A or C. To view the data type correlated to validation criteria, see "Device Templates Overview" on page 462

    > **NOTE:** If values are already displayed on the Validation tab, they provide the range that governs the default values you set for the definition. The operator sees only the validation criteria and their values if you supply them when you create an error message. You do not always need to enter any character on the Validation tab. However, in certain cases, input is mandatory—for example, when a hostname is to be validated.

20. To modify the details on the Validation tab, click the **Validation** tab.

21. Enter the parameters for the option in the appropriate fields.

    If the fields already display default values and you change them, ensure that your values do not exceed the default values.

    The Regular Expression Error Message box on the Validation tab appears only if you configure an option of the string data type.

22. (Optional) For a string, in the **Regular Expression** field, enter a regular expression to further restrict what the operator can enter.

23. (Optional) For a string, compose an error message.

    This is not a validation parameter but rather a clue to enable the operator to enter correct field data. The text you enter here is displayed when an operator enters invalid content in a template field. An error message is very helpful for ensuring that operators are successful in creating templates. You cannot enter an error message if you have not entered a regular expression.

24. To save your entries, select another tab or another option, or click **Next**.

    The settings on the Advanced tab determine whether:

    - The operator can see the selected option or edit its values.
    - Device-specific values are used for the selected option. The Device Specific check box appears only for options of these data types:
        - Integer
        - String
        - Boolean
        - List

25. To modify the details on the Advanced tab, select the **Advanced** tab.

26. Select **Editable**, **Readonly**, or **Hidden**, depending on whether the operator creating the device template should see this device configuration parameter, or change it.

    If you hide an option, the operator can see neither the settings for the option nor the option itself.

27. (Optional) To mark this configuration option as device specific, click the **Device Specific** check box.

    See"Specifying Device-Specific Values in Template Definitions" on page 482 for further instructions on using CSV files for this purpose. You can use rules instead of or in addition to CSV files to specify device-specific values. See "Working with Rules in a Template Definition" on page 480 for more information about working with rules in a template definition.

28. To save your entries, select another tab or another option, or click **Next**.

29. To specify default values for configuration options, select the configuration option.

30. (Optional) To add comments for individual parameters, click the little yellow comment icons next to the configuration settings and enter your comments.

31. (Optional) To activate or deactivate a configuration option, click the **Activate** or **Deactivate** link respectively.

> **NOTE:** You can activate or deactivate a configuration option only if the configuration node exists.

32. To display the fields for the default values, click **View/Configure**.

    The layout of the fields on the page varies depending on the data type of the configuration option you selected. For more details, see the "Finding Configuration Options in a Template Definition" on page 478 topic.

33. To add a row to a table, click the plus sign (+).

    The fields for the options displayed in the previous view appear. Whether the operator can edit the option values depends on the settings you made on the Advanced tab: Editable, Readonly, or Hidden.

    To remove a row from a table, select the row and click the minus sign (–). To edit a table row, select the row and click the pencil icon .

    As you drill down, successive breadcrumbs appear, with the names of the options you clicked to configure, enabling you to navigate through multiple configuration option levels. The operator also sees these breadcrumbs and uses them to navigate.

34. Enter the data as appropriate.

> **TIP:** To review your settings, click **Back** at the bottom of the page.
>
> Any field that you have marked as editable can remain empty, but do not leave hidden and read-only fields empty.

    If you enter an invalid value, a red exclamation mark icon appears. Click the icon to find out what the value should be. The same icon is also visible to the operator when creating a template.

    Click the blue Information icon on the far right of each setting to view the explanatory or descriptive text for the operator that you entered on the Description tab.

35. (Optional) To view what the operator sees, click **Operator View**.

36. (Optional) Add settings in the Operator View.

    When you click **Designer View**, a message appears, asking “Do you want to save this draft before you leave this page?”

37. (Optional) To save the settings you made in the Operator View, click **Yes**.

38. To complete your definition, return to the designer view by clicking **Designer View** .

39. Click **Finish**

RELATED DOCUMENTATION

Device Templates Overview | 462

Creating a Device Template | 494

Finding Configuration Options in a Template Definition

You can locate configuration options in a template definition in two ways: you can browse the list of configuration options or use the search functionality.

To display the top level configuration options, click the plus sign [+] or expansion icon at the top of the tree in the Available Configuration area. Many of the configuration options contain more parameters. To display these, click on the plus sign [+] or expansion icon on the left of the configuration option.

To search for a specific configuration option:

1. Click the magnifying glass icon.

   The Search field appears.

2. Enter your search term.

   As soon as you enter the first three letters, the Search field opens downwards, displaying the search results.

   Search field displays only the first ten matches for your term.

TIP: Search results appear while you are typing. You can continue typing or even delete text. The cursor might not be visible in the Search field if the focus is somewhere within the list of search results.

The order of the search results is not dependent on the order of those items in the Available Configuration area. The order is based on the similarity of your search term to the indexed fields.

3. You can select a result in three ways:
   1. Using the mouse to click on it.
   2. Pressing the Enter key to select the first result in the list.
   3. Using the up and down arrow keys on the keyboard to move through the list, pressing the Enter key to select a result.

   The tree in the Available Configuration area jumps to the location of the match for the result you selected and highlights the configuration option. The list of results disappears.

4. (Optional) To review the results that you did *not* select, either:
   - Click the white arrows next to the Search field.

     Click the arrow to the left to move to the result listed previous to the selected result.

     Click the arrow to the right to move to the resulted after the selected result.
   - Use the left and right arrow keys on the keyboard.

     Press the arrow to the left to move to the result listed previous to the selected result.

     Press the arrow to the right to move to the resulted after the selected result.
5. To close the Search field, click X in the right corner of the Search field.

RELATED DOCUMENTATION

Device Templates Overview | 462

Working with Rules in a Template Definition | 480

Creating a Template Definition | 471

Working with Rules in a Template Definition

Device Templates uses rules to supplement the device-specific value capability supplied by CSV files. Specify rules to resolve device specific values at the time of deployment. You can use rules in addition to CSV files, or instead of CSV files. The system resolves device specific values by first checking the CSV file and then the rules. If both the CSV file and the rules return a value, the CSV file takes precedence. If neither the CSV file nor the rules return a value, deployment validation will fail. If a rule cannot provide the requisite value, the operator will be prompted to enter it at deployment.

The system resolves device specific values by first checking the CSV file and then the rules. If both the CSV file and the rules return a value, the CSV file takes precedence. If neither the CSV file nor the rules return a value, deployment validation will fail. If a rule cannot provide the requisite value, the operator will be prompted to enter it at deployment.

Rules are applied in the order shown. You can change the order as necessary. You can create rules for devices whose names start with a specific word, or rules for devices with a specific tag.

You can add, edit, move, and delete rules. You can only select one rule at a time.

To add a rule:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

   The Definitions page is displayed.

2. Click the **Create Template Definition** icon on the Actions bar.

   The Create Template Definition page is displayed.

3. Add the configuration option for which you want to supply device-specific values using a CSV file that you have already created.

4. Click the **Advanced** tab.

5. Select the **Device Specific** check box.

6. Click **Next**.

7. Click **Please select a CSV file**.

   The Manage CSV files pop-up window is displayed.

   Use the Manage CSV files workflow to either select a file already in the system, or to navigate and upload CSV files from the local file system. You can view the content of a CSV file already in the system by selecting it in the left pane. Its content displays in the right pane.

8. To use a CSV file already in the system, select it and click **OK**.

9. Specify the column and the key column in the CSV file.

10. Select the **Resolve the value from a CSV file at deploy time** check box.

    You can now add rules.

11. Click the [+] icon.

    Two options appear:

    - Rule matching tagged device
    - Rule matching device name.

12. Select the appropriate option.

    A rule appears, depending on your selection in the previous step, either of the following:

    - Set to a specific value for devices tagged with a specific tag
    - Set to a specific value for devices with name starting with a specific word.

    In both cases, the phrase “a specific value” is a link, as are “a specific tag” and “a specific word.”

13. Click either **a specific tag** or **a specific value**.

    The **Set $dsv** field appears.

14. Enter the appropriate value.

    If the value you enter is not valid, an error message appears in the form of a tool tip explaining why the entry is invalid.

15. To save your input, click the **OK** button. To clear your input, click the [X] button.

    The rule reappears, this time with your input replacing the link.

16. (Optional) To change the sequence of in which the rules will be applied, select a rule and click either the up arrow icon or the down arrow icon.

    The selected rule moves to the new position.

17. (Optional) To delete a rule, select the rule and click the [X] button.

    The selected rule disappears.

18. (Optional) To clone a rule, select the rule and click the last icon on the right, next to the down arrow.

A clone of the selected rule appears.

19. (Optional) Refresh the rules display by clicking the Refresh icon in the lower bar of the Rules section of the Device Specific Value dialog.

20. When you have finished working with rules, close the Device Specific Value dialog box by clicking **Close**.

RELATED DOCUMENTATION

Device Templates Overview | 462
Creating a Template Definition | 471

Specifying Device-Specific Values in Template Definitions

IN THIS SECTION

Creating a CSV file with device-specific values | 482
Using a CSV file to set device-specific values | 483

Template designers can use a comma-separated value (CSV) file to provide device-specific values for a template definition. A single CSV file can be used to supply as many values as you wish, because the same file can be used again. Once you have created a CSV file, you import it into Junos Space Network Management Platform , and manage it using the Manage CSV Files task in the Device Templates workspace.

Creating a CSV file with device-specific values

You create a CSV file to import the device-specific values into a template definition. Use one column for each value to be specified and use one row for each device.

To create a CSV file:

1. Open an appropriate program such as Notepad or Microsoft Excel.

2. Create a header row to name your columns.

It does not matter what you name your columns - you could call them anything, but each name must be unique, because Junos Space Network Management Platform uses them to identify the values for the template definition.

If you wanted the value **sac-contact** in your definition, you would need to specify the column **Contact**, while the key column would be **Sacramento**.

3. If you wanted to specify interfaces and other values, you would simply add a column for each type of value, which specifies two interfaces on a single device, as well as MTU and traps for each.

> **NOTE:** You must correctly identify the column from which the value is to be taken and the key column when you select the CSV file during the template definition creation process. You do not necessarily need to note down this information, because you can view the contents of the CSV file in Junos Space Network Management Platform when you choose column and key column.

4. Save the CSV file on your system.

Using a CSV file to set device-specific values

You use the CSV file to set device-specific values in a template definition.

To use a CSV file to set device-specific values in a template definition:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

   The Definitions page is displayed.

2. Click the **Create Template Definition** icon on the Actions bar.

   The Create Template Definition page is displayed.

3. Add the configuration option for which you want to supply device-specific values using a CSV file that you have already created.

4. Click the **Advanced** tab.

5. Select the **Device Specific** check box.

6. Click **Next**.

7. Click the **Device Specific Value** link.

   The Device Specific Value - Authorization pop-up window is displayed.

8. Select the **Resolve the value from a CSV file at deploy time** checkbox.

9. Click **Please select a CSV file**.

   The Manage CSV files pop-up window is displayed.

   Use the Manage CSV files workflow to either select a file already in the system, or to navigate and upload CSV files from the local file system. You can view the content of a CSV file already in the system by selecting it in the left pane. Its content displays in the right pane.

10. To use a CSV file already in the system, select it and click **OK**.

11. Specify the column and the key column in the CSV file.

12. Select the **Resolve the value from a CSV file at deploy time** check box.

    You can now add rules. See "Working with Rules in a Template Definition" on page 480 to know how to add, delete, and move rules.

13. Click **Finish**.

RELATED DOCUMENTATION

Device Templates Overview | 462

Creating a Device Template | 494

Managing CSV Files for a Template Definition

Device Templates uses CSV files to specify device-specific values, in addition to rules (see "Working with Rules in a Template Definition" on page 480). The Managing CSV Files task describes how to import this type of CSV file into Junos Space Network Management Platform. For instructions on the procedure for linking the file to a definition and identifying the key column for Device Templates, see "Specifying Device-Specific Values in Template Definitions" on page 482.

Although designers can configure the parameter governed by the CSV file as editable, operators can neither view nor change the file when they create templates.

The CSV files you use can be any file format (for example, .xls or .txt) as long as they have appropriate columns and key columns. That means one row per device. If you want to reference several interfaces on a single device, then each of the interfaces must have its own column.

You can add a record to a CSV file from within Device Templates. However, if you change a CSV file outside Junos Space Network Management Platform, from its native application (for example, Microsoft Excel or Notepad), you must upload it again. You can do this within the device templates workflow.

To add the CSV files:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

   The Definitions page is displayed.

2. Click the Manage CSV Files icon on the Actions bar.

   The Manage CSV File page is displayed.

3. Click **Upload**.

   The CSV File upload pop-up window is displayed.

4. Click **Browse**.

   The File Upload pop-up window is displayed.

5. Navigate to the desired CSV file, select it and click **Open**.

6. Click **Upload**.

   The Manage CSV Files page is displayed. The name of the file just imported appears in the left pane.

7. To display the content of a file, select its name in the left pane.

RELATED DOCUMENTATION

Device Templates Overview | 462
Creating a Template Definition | 471

Publishing a Template Definition

You publish a template definition when you want to make it available to create device templates from the template definition.

To publish a template definition:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

   The Definitions page is displayed.

2. Select the template definition you want to publish and select **Publish Template Definition** from the Actions menu.

   The Publish Template Definition page is displayed.

3. Click Publish.

RELATED DOCUMENTATION

Device Templates Overview | 462
Unpublishing a Template Definition | 492

Viewing a Template Definition

You view a template definition when you need to view the details of the template definition.

To view a template definition:

1. On the Network Management Platform user interface, select **Device Templates > Definitions**.

   The Definitions page that appears displays the template definitions.

2. Select the template definition you want to view and select the **View Template Definition Details** icon from the Actions bar.

   The View Template Definition dialog box is displayed.

   Table 52 lists the details of the template definition displayed in the View Template Definition dialog box.

   Table 52: View Template Definition Dialog Box Details

Field or Area	Description	Displayed In
Name	Name of the template definition	Definitions page View Template Definition dialog box
Description	Description of the template definition	Definitions page View Template Definition dialog box
Device Family	Device family to which the template definition belongs	Definitions page View Template Definition dialog box
OS Version	OS version to the template definition	View Template Definition dialog box
Available Configuration area	Configuration options of the device family chosen for the template definition	View Template Definition dialog box
Selected Configuration Layout area	Details of the configuration options in the template definition	View Template Definition dialog box

3. Click **Next**.

   The View Template Definition dialog box displays the default values for the configuration parameters. You can switch between designer and operator views.

4. Click **Finish** to close the View Template Definition dialog box.

RELATED DOCUMENTATION

Modifying a Template Definition | 488
Cloning a Template Definition | 489
Creating a Template Definition | 471
Device Templates Overview | 462

Modifying a Template Definition

You modify a template definition when you want to propagate the configuration changes to the device template. You cannot change the device family, OS version, and schema version when modifying the original template definition. When you modify a template definition, you cannot change any existing configuration pages. You can only add new configuration pages.

> **NOTE:** You cannot modify a template definition if the template definition is published. You should first unpublish the template definition before modifying it. If you try to modify a template definition without unpublishing, an error message will be displayed.

To modify a template definition:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

   The Definitions page is displayed.

2. Select the template definition you want to modify and click the Modify Template Definition icon on the Actions bar.

3. Modify the parameters you want to modify.

4. Click **Finish**.

   After you modify the template definition, republish the associated device templates.

RELATED DOCUMENTATION

Device Templates Overview | 462
Creating a Template Definition | 471

Cloning a Template Definition

You clone a template definition to quickly create a new template definition with a new name but same properties.

To modify a template definition without disabling templates based upon that definition, first clone the definition, then modify the clone.

Unlike the **Modify** function, the **Clone** function does not require that a definition be unpublished.

When you clone a template definition, you cannot change the device family or any existing pages.

To add additional pages, modify the clone (see "Modifying a Template Definition" on page 488).

To clone a template definition:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

   The Definitions page is displayed.

2. Select the template definition you want to clone and select **Clone Template Definition** from the Actions menu.

   The Clone Template Definition pop-up window is displayed.

3. (Optional) In the **Please specify a new name for the clone** field, enter a user-defined template definition name.

   If you do not enter a new name for the template definition, Junos Space Network Management Platform creates the new template definition by appending "clone of" to the original template definition name.

4. (Optional) In the **Description** field, enter a user-defined description.

5. Click **Clone**.

RELATED DOCUMENTATION

Device Templates Overview | 462

Creating a Template Definition | 471

Importing a Template Definition

You can import template definitions from XML files and export template definitions to XML files. A template definition retains its state when it is exported or imported; published template definitions that are exported also appear as published when they are imported. Therefore, if you import a template definition that was published, but do not want it to be available to operators, you must unpublish it either before you export it or immediately after importing it. You can transfer template definitions from one Junos Space fabric to another.

A template definition is based on a specific OS version, or DMI schema . If the template definition you import is based on a schema that is not found, the template definition is set to the default DMI schema assigned to the device family to which the template definition applies. If you have not set the default schemas for your device families, Junos Space Network Management Platform defaults to the most recent schema for each.

Before you begin, make sure you have access to a template definition file. Although it is an XML file, the system expects to find it packed into a .tgz file, which is the way the system exports XML files (see "Exporting a Template Definition" on page 491).

To import a template definition:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

   The Definitions page is displayed.

2. Select the Import Template Definition icon on the Actions menu.

   The Import Template Definition page is displayed.

3. To locate a definition file, click the **Browse** button.

   The File Upload dialog box opens.

4. Navigate to the appropriate file, select it, and click **Open**.

   The Import Definition dialog box reappears, displaying the name of the selected file in the Definition File box.

> **NOTE:** Under some circumstances, when the **Import Definition** dialog box reappears, it displays a message beginning with the phrase “Confirm name mapping of.” This message serves as a warning that the system has changed the name mapping on the CSV file associated with the imported template definition, and the name of the template definition.

5. Click **Import**.

RELATED DOCUMENTATION

Device Templates Overview | 462
Exporting a Template Definition | 491

Exporting a Template Definition

You export a template definition when you want to transfer this template definition to another Junos Space fabric. A template definition retains its state when it is exported.

To export a template definition:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

   The Definitions page is displayed.

2. Select the template definition you want to export and select **Export Template Definition** from the Actions menu.

   The Export Template Definition pop-up window is displayed.

3. Click **Download file for selected template definitions (tgz format)**.

   The Opening xxx.tgz dialog box appears. (XXX is a placeholder for the name of the template definition.)

4. Select **Save File** and click **OK**.

   You may have to toggle between the option buttons to activate the **OK** button.

   The Enter name of file to save to ... dialog appears.

5. Rename the file if desired and save it to the appropriate location.

   The Export Template Definition dialog reappears.

6. Click **Close**.

   Although the exported definition file is an .XML file, it is saved as a .tgz file, which is the format the system uses to import XML files.

RELATED DOCUMENTATION

Device Templates Overview | 462

Importing a Template Definition | 490

Unpublishing a Template Definition

You unpublish a template definition when you do not want to use it to create device templates or when you want to deactivate the device templates that are created based on the template definition.

To unpublish a template definition:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

   The Definitions page is displayed.

2. Select the template definition you want to unpublish and select **Unpublish Template Definition** from the Actions menu.

   The Unpublish Template Definitions dialog box is displayed. You can view the device templates that use this template definition.

   NOTE: If you unpublish a template definition with which templates are associated, the templates are disabled for deployment and further use until you publish the template definition.

3. Click **Unpublish**.

   The template definition is unpublished. You are redirected to the Template Definitions page.

RELATED DOCUMENTATION

Device Templates Overview | 462

Publishing a Template Definition | 486

Deleting a Template Definition

You delete a template definition when you no longer need the template definition to propagate the configuration changes to the device template. You can delete a template definition only when it is unpublished.

NOTE: When you delete a template definition, all device templates based on that template definition are permanently disabled. You cannot modify or deploy such templates.

To delete a template definition:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Definitions**.

   The Definitions page is displayed.

2. Select the template definition you want to delete and select the Delete Template Definition icon on the Actions bar.

   The Delete Template Definitions pop-up window is displayed.

3. Click **Delete**.

RELATED DOCUMENTATION

Device Templates Overview | 462

Creating a Template Definition | 471

CHAPTER 27

Configuring Devices using Device Templates

IN THIS CHAPTER

- Creating a Device Template | 494
- Assigning a Device Template to Devices | 496
- Deploying a Template to the Devices | 498
- Modifying a Device Template | 502
- Undeploying a Device Template from the Devices | 503
- Unassigning a Device Template from the Devices | 504
- Auditing a Device Template Configuration | 505

Creating a Device Template

Device templates enable operators to update the Junos OS configuration running on multiple Juniper Networks devices at once. The operators can create and deploy device templates based on template definitions created by designers from the Device Templates workspace.

To create a device template:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

   The Templates page is displayed.

2. Click the Create Template icon on the Actions bar.

   TIP: The Create Template page is displayed. This page lists all the template definitions. The operators can only see published template definitions. If you do not see a template definition that you expect to see, the designer might have unpublished it.

3. Select a template definition and click **Next**.

4. In the **Template Name** field, enter a user-define name for the device template.

The template name is required. The template name must be unique and limited to 63 characters.

5. (Optional) In the **Description** field, enter a user-defined template description.

   The template description is optional and limited to 255 characters.

6. Select a configuration page.

   The breadcrumb of that page is displayed on the right side of the page. The configuration options are displayed in the pane below the breadcrumbs.

   > **TIP:** To navigate through the configuration options on any page, click the breadcrumbs.
   >
   > As you drill down, successive breadcrumbs appear, with the names of the options you clicked to configure. You can navigate through multiple configuration option levels.
   >
   > The layout of the configuration settings on the page varies depending on the data type of the configuration option selected.

7. (Optional) For information on the individual parameters, click the little blue information icons to the right of the configuration settings to display the explanations the designer wrote.

8. (Optional) To add comments for individual parameters, click the little yellow comment icons next to the configuration settings and enter your comments.

9. (Optional) To activate or deactivate a configuration option, click the **Activate** or **Deactivate** link respectively.

   > **NOTE:** You can activate or deactivate a configuration option only if the configuration node exists.

10. (Optional) Add any required configuration specifics.

    You can change only configuration options that the definition designer made editable.

    > **NOTE:** You must click through all the settings to ensure that all necessary values are populated.

11. (Optional) To add a row to a table, click the plus sign (+).

To remove a row from a table, select the row and click the minus sign (-). To edit a table row, select the row and click the pencil icon (looks like a diagonal line).

12. Enter the data, as appropriate.

    If you enter an invalid value, a red exclamation mark icon appears. Click the icon to find out what the value should be.

13. Click **Finish**.

RELATED DOCUMENTATION

Device Templates Overview | 462

Creating a Template Definition | 471

Assigning a Device Template to Devices

You assign a device template to devices to set up this device template for deployment. When you assign a template to devices, the device template is placed in the queue to deploy to devices. You can review the accumulated configuration changes that are in the queue to be deployed to the device. A device template that has been assigned to a device cannot be deployed directly. You can use this workflow to assign both configuration templates and quick templates.

> **NOTE:** The chassis cluster devices discovered using the fxp interface are treated as separate units when assigning a device template. It is same for logical systems and virtual chassis configuration setups as well. In such scenarios, select the primary node or the primary node of the setup to deploy the template.

To assign a device template to devices:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

   The Templates page is displayed.

2. Select the configuration template or quick template to be assigned, and select **Assign to Device** from the Actions menu.

   The Assign to Device page is displayed. You can view the list of compatible devices, that is, those devices that belong to the same device family as the device template.

3. From the **Selected Template Version** drop-down list, select the version of the device template that you want to assign to devices.

4. You can assign the device template to devices manually, using tags, or by providing a CSV file with filter criteria.

   - To assign the device template to devices manually, search for compatible devices by entering the search criteria in the search box and clicking the magnifying glass icon.

     The list of devices are filtered by the search criteria.

   - To filter devices by the device properties, select the check box next to the appropriate device column on the **Column Filter** drop-down list.

   - From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.

     To provide filter criteria using a CSV file, click the CSV Filter icon and upload the CSV file with filter criteria through the Upload a CSV pop-up window.

   - To select a device by using tags, select an appropriate tag from the **Tag Filter** drop-down list.

5. Click **Next**.

6. From the left section, select the devices to which you want to assign the device template.

7. On the right section, click **XML** or **CLI** tabs to view the XML and CLI formats of the configuration in the device template.

8. Click the **Validate on Device** link to validate the configuration on the device.

   By validating the configuration, you ensure that the device template is semantically correct. If the validation results fails, change the template parameters appropriately.

   If the validation succeeds, the Validation Status column in the left section displays a SUCCESS status.

9. Click **Assign**.

   The device template is assigned to devices. You are redirected to the Templates page.

Release History Table

Release	Description
17.2	From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.

RELATED DOCUMENTATION

Device Templates Overview | 462

Unassigning a Device Template from the Devices | 504

Deploying a Template to the Devices

You deploy a template to the devices to update the configuration on the devices. Before deploying a template to a device, ensure that you have not already assigned the template to the same device. If you assign a template to a device and use the Deploy workflow to deploy that template on the same device, even if the template is deployed to the device, Junos Space Network Management Platform does not reflect this managed status. The managed status of the device is shown as "Space Changed" on the Device Management page.

You can also use this workflow to assign and publish the template to the devices. You assign and publish a template to the devices to set up this template for deployment. When you assign and publish a template to the devices, the template is placed in queue. You can review the accumulated configuration changes that will be deployed to the devices.

To deploy or assign a template to the devices:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

   The Templates page is displayed.

2. Select the device template that you want to deploy and select **Assign/Deploy Template** from the Actions menu.

   The Assign/Deploy Template page is displayed. This page displays the devices on which the template can be deployed.

3. From the **Selected Template Version** drop-down list, select the version of the device template that you want to deploy or assign to the devices.

4. You can deploy the device template by selecting the devices manually, filtering by device properties, using tags, or providing a CSV file with filter criteria:

   - To select the devices manually, enter the search criteria in the Search field and click the Search icon.

     The list of devices are filtered by the search criteria.

   - To filter devices by device properties, select the check box next to the appropriate device column on the **Column Filter** drop-down list.

- To select a device by using tags, select an appropriate tag from the **Tag Filter** drop-down list.
- From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.

  To provide filter criteria using a CSV file, click the CSV Filter icon and upload the CSV file with the filter criteria through the Upload a CSV pop-up window.

5. Select the devices on which you want to deploy the template and click **Next**.

   This page displays the devices you chose on the left and the configuration to be deployed on the device on the right. You can also view details such as device name, managed status, validation status.

   If you specified device-specific values when creating the template definition, the Variable column is displayed. This column displays the validity of the value of the device-specific variable: PASS or FAIL.

6. (Optional) To validate the configuration on the device before deploying, select the device and click the **Validate on Device** link.

   By validating the configuration, you ensure that the device template is semantically correct. If the validation fails, change the template parameters appropriately.

   > **NOTE:** If you select modeled devices that are in the Modeled state, the Validate on Device link is disabled.

   A job is triggered. You can view the details of the job from the Job Management page. When the job is completed, the job ID is displayed next to the Validate on Device link.

   > **NOTE:** If validation fails on all devices you selected, you cannot deploy the template on devices. If validation fails on some devices you selected, you can deploy the template to only those devices that succeeded the validation.

7. (Optional) To view the XML format of the configuration, select the device and click the **XML** tab.

8. (Optional) To view the CLI format of the configuration, select the device and click the **CLI** tab.

9. Click **Next**.

10. Select whether to deploy the device template now or later or whether to only assign and publish it.

    - To assign and publish the device template, select the **Assign and Publish to pending configuration changes** option button.

- To deploy the device template now, select the **Deploy Now** option button.
- To deploy the device template later:
  a. Select the **Deploy Later** option button.
  b. Enter the date in the **Date** field in the DD/MM/YYYY format.
  c. Enter the time in the **Time** field in the hh:mm format.

> **NOTE:** If you select modeled devices that are in the Modeled state, the Deploy Now and Deploy Later buttons are disabled.

> **NOTE:** If you publish the template, the configuration in the template is deployed to the device along with the candidate configuration for the device, with the Junos OS confirmed-commit functionality.

11. Click **Finish**.

    The Deploy Template Job Information page is displayed. You are redirected to the Templates page.

Click **OK** to close the page.

The device template is deployed to the devices.

> **NOTE:** You can check whether a template is deployed on all devices from the Job Management page. Double-click the row corresponding to the ID of the device template deployment job on the Job Management page. The Job Details page is displayed. The Description column on this page specifies whether the template is deployed on all devices. If the device template is not deployed on all devices, this column lists the reason why the template was not deployed. If there is an error, the View Job Details page displays an error message. For more information about the error messages, see "Common Error Messages in Device-Related Operations" on page 992.

NOTE: If you deploy the template when in SSOR mode, Junos Space Network Management Platform automatically assigns the template to the device. To subsequently modify the template, use one of the following workflows:

- Unassign the template from the device, modify the template, and deploy the template by using the Deploy workflow.
- Modify, approve, and deploy the template on the device by using the Review/Deploy Configuration workflow in the Devices workspace.

Release History Table

Release	Description
17.2	From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.

RELATED DOCUMENTATION

Device Templates Overview | 462

Viewing the Device-Template Association (Device Templates) | 521

Undeploying a Device Template from the Devices | 503

Modifying a Device Template

You modify a device template to propagate the modifications to the device to which the device template is assigned. If you need to modify the device template after deploying the device template, the template designer must check the device template and the template definition to fix any errors. You should redeploy the device template only after the errors are fixed. You can use this workflow to modify both Configuration templates and Quick templates.

> **NOTE:** A new version of the template is created if you modify a template that is in the Assigned or Deployed state.

To modify a device template:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

   The Templates page is displayed.

2. Right-click the device template that you want to modify and select Modify Template.

   The Modify Template page is displayed.

3. Modify the device template name, description, or configuration settings.

4. Click **Modify**.

   The template is modified. You are redirected to the Templates page.

RELATED DOCUMENTATION

Device Templates Overview | 462

Creating a Device Template | 494

Undeploying a Device Template from the Devices

You undeploy a device template from the devices to remove the configuration changes pushed to the devices when the device template was deployed. You can use this workflow to undeploy a Configuration template or Quick template from the devices.

To undeploy a template from the devices:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

   The Templates page is displayed.

2. Select the template that you want to undeploy and select **Undeploy Template** from the Actions menu.

   The Undeploy Template page is displayed. This page displays details such as the devices on which the template is currently deployed, the Device Alias custom label of the device, version of the template deployed and assigned to the devices, and IP addresses of the devices.

3. Select the devices from which you want to undeploy the template.

4. Click **Next**.

   The Review Changes page is displayed. This page displays the devices on the left of the page. The right of the page displays the configuration changes that result from undeploying the template from a selected device.

5. Select a device from the left of the page.

6. (Optional) To view the summary of the changes when the template is undeployed from the selected device, click the **Change Summary** tab.

7. (Optional) To view the device's current configuration, click the **Deployed** tab.

8. (Optional) To view the audit status of the deployment of this template to the device, click the **Audit Result** tab.

9. Click **Next**.

   The Confirm Undeployment page is displayed.

10. Select whether to undeploy the device template now or later.

    - To undeploy the template now, click **Finish**.
    - To undeploy the template later:

a. Select the **Schedule at a Later Time** option button.

b. Enter the date in the **Date** field in the DD/MM/YYYY format.

c. Enter the time in the **Time** field in the hh:mm format.

d. Click **Finish**.

The template is undeployed from the devices. You are redirected to the Templates page.

> **NOTE:** View job details if a device template is not undeployed from all the devices even after using the Undeploy workflow. The Description column on the Job Details page specifies why the template was not undeployed from all the devices.

RELATED DOCUMENTATION

Device Templates Overview | 462

Deploying a Template to the Devices | 498

Unassigning a Device Template from the Devices

You unassign a template from the devices if you do not want to deploy it to the devices. Then this template is no longer part of the consolidated configuration changes. You can use this workflow to unassign both Configuration templates and Quick templates.

To unassign a device template from the devices:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

   The Templates page is displayed.

2. Select the devices from which you want to unassign the template and select **Unassign from Device** from the Actions menu.

   The Unassign from Device page is displayed. You can view the device names, the Device Alias custom labels of the devices, IP address of the devices, versions of the template assigned to the devices, and versions of the template deployed to the devices.

3. Click **Next**.

The Confirm Unassignment page is displayed.

4. Click **Finish**.

   The Template Unassign Confirmation dialog box is displayed. You are redirected to the Templates page.

Click **OK** on the dialog box.

The template is unassigned from the devices.

RELATED DOCUMENTATION

Device Templates Overview | 462
Assigning a Device Template to Devices | 496

Auditing a Device Template Configuration

You audit the configuration in the template that is already deployed to the devices. You perform an audit to verify the extent to which the configuration in the template and that on the deployed devices match. You can use this workflow to audit both Configuration templates and Quick templates.

To audit a template configuration:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

   The Templates page is displayed.

2. Select the template whose deployment you want to audit and select **Audit Template Configuration** from the Actions menu.

   The Audit Template Configuration page is displayed. You can view the name of the template, current selected version of the template, Junos OS version of the template, and devices that belong to the same device family. The **Include All Managed Devices** check box ix selected by default. Clear this selection to list only those devices that are UP and INSYNC states if you select **All** in the **Selected Template Version** drop-down list. If you select a specific template version, all devices that have the specified version of the template deployed and are in UP or INSYNC states are listed.

3. (Optional) From the **Selected Template Version** drop-down list, select the version of the template.

   The list of devices displayed is filtered according to the version of the template you select in this field. The list is filtered to display only those devices on which the template is currently deployed.

4. You can select devices manually, by filtering devices by device properties, by using tags, or by providing a CSV file with filter criteria:

   - To search for devices manually, enter the search criteria in the Search field and click the Search icon.

     The list of devices are filtered by the search criteria.

   - To filter devices by device properties, select the check box next to the appropriate device on the **Column Filter** drop-down list.
   - To select devices by using tags, select an appropriate tag from the **Tag Filter** drop-down list.
   - From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.

     To provide filter criteria through a CSV file, click the CSV Filter icon and upload the CSV file with the filter criteria by using the Upload a CSV pop-up window.

5. Click **Next**.

   The devices you selected are listed on the left of the page.

6. Select whether to audit the template configuration against the configuration in devices now or later:

   - To audit the template configuration against the configuration in devices now, click **Finish**.
   - To schedule this task for a later time:

     a. Select the **Schedule at a later time** option button.

     b. Enter the date in the **Date** field in DD/MM/YYYY format.

     c. Enter the time in the **Time** field in hh:mm format.

7. (Optional) Click the **Recurrence** check box and specify the frequency at which to audit the device template configuration against the configuration in the devices.

8. Click **Finish**.

   The Audit Template Job Information page is displayed.

9. Click **OK** to close the page.

   You are redirected to the Templates page.

   To view the results of the job triggered for this auditing, click the job ID on the Audit Template Job Information page. You are redirected to the Job Management page with a filtered view of the job. Double-click the row corresponding to the job to view the detailed status of the job on the Compare Config Job Status page. For devices that are OUTOFSYNC or DOWN, the summary of the job displays a warning message.

To export the report of auditing the template configuration, click the **Export** button. You are prompted to save the file. Click **OK** on the File Save page to save the file.

The details of the auditing job, along with the warning message, are listed in the exported report.

After you save the file, to return to the Job Management page, click the [X] icon on the Compare Config Job Status page.

> **NOTE:** Each audit is performed as a job. It might take some time to finish auditing if a large number of devices was selected for auditing.

The possible statuses for a template audit are:

- **INSYNC**— The configurations in the template and on the device are the same.
- **OUTOFSYNC**— The configuration in the template is different from that on the device.
- **NOTAVAIL**— The configuration in the template is not available on the device. This status is displayed when no audit is performed on a device for a particular template.

You can view these statuses in the Summary column on the Job Management page.

Release History Table

Release	Description
17.2	From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.

RELATED DOCUMENTATION

Device Templates Overview | 462

Creating a Device Template | 494

Deploying a Template to the Devices | 498

CHAPTER 28

Configuring Devices using Quick Templates

IN THIS CHAPTER

- Quick Templates Overview | 508
- Creating a Quick Template | 509
- Deploying a Quick Template | 515

Quick Templates Overview

With the Quick Template feature, you can use a CLI-based template editor or a form-based editor to send configuration details to multiple devices. You can switch between the two editors to specify the configuration that you want to send. A configuration added from the form-based editor appears in the CLI-based template editor in CLI format and a configuration element added from the CLI-based editor appears as a form in the form-based editor.

During Quick template creation, you can set default values for variables in the configuration elements and reorder these variables. You use the revised order to display variables when you resolve these variables before deploying them. You can save the variable settings in a CSV file and download it to your local computer.

You can deploy Quick templates on devices by manually selecting devices; by filtering devices by their properties such as device name, connection status, managed status, Junos OS version, IP address, and platform, by tags, or by providing a CSV file with filter criteria. Before you deploy the configuration to the devices, resolve the variables in the configuration elements manually, using tags, or by uploading a CSV file that specifies how to resolve the variables. You can choose to deploy the configuration immediately, or at a later time, or only publish the Quick template.

You can export and import Quick templates in XML format. You can create a Quick template based on the current configuration on a managed device by using the Create Template from Device Configuration workflow (**Devices > Device Management > Device Configuration > Create Template from Device Configuration**) from the Devices workspace.

You cannot copy the configuration from the CLI-based template editor directly to the CLI console of a device. To successfully copy and commit the configuration, copy the configuration from the CLI-based template editor to a text file before copying the configuration to the CLI console of a device.

> **NOTE:** You can erase the configuration from a device by using Quick templates. To do so, replace the SET commands with DELETE commands by using the CLI-based Template editor and deploy the Quick template to the device. Then the configuration is erased from the device. If you undeploy the Quick template from the device, the configuration is reset.

RELATED DOCUMENTATION

- Creating a Quick Template | 509
- Deploying a Quick Template | 515
- Exporting and Importing a Quick Template in Junos Space Network Management Platform | 530

Creating a Quick Template

You create a Quick template to push a configuration to the devices. A Quick template is a device template created without a template definition.

> **NOTE:** To create a Quick template based on the current configuration on a managed device by using the Create Template from Device Configuration workflow, click **Devices > Device Management > Device Configuration > Create Template from Device Configuration** from the Devices workspace. You are directed to the Create Quick Template page.

To create a Quick template:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

   The Templates page is displayed.

2. Click the Create Template icon on the toolbar and select **Create Quick Template**.

   The Create Quick Template page is displayed.

3. In the **Name** field, enter a name for the Quick template.

   The Quick template name is required. The Quick template name must be unique and contain at most 63 characters.

4. (Optional) In the **Description** field, enter a description of the Quick template.

   You can enter at most 255 characters.

5. From the **Device Family** drop-down list, select an appropriate device family.

6. From the **Versions** drop-down list, select an appropriate Junos OS version.

7. You can create a Quick template by using the CLI-based template editor or the form-based template editor.

   To create a Quick template by using the CLI-based template editor:

   a. Click the **CLI-based Template Editor** link.

      The Template Editor dialog box is displayed. To the left of the Template Editor is a text-editing area. You can type or paste Junos OS CLI commands in the text-editing area. A toolbar at the top of the text-editing area provides functionalities such as save, syntax validation, copy, paste, cut, undo, redo, and find. To the right area of the Template Editor configuration options, such as Access profile, Class of service, and Firewall are provided. The device family that you select determines which configuration options are displayed.

      > **NOTE:** In Google Chrome and Internet Explorer browsers, the keyboard shortcuts and the tool bar options for cut, copy, and paste may not work at times. If you encounter this issue, use the right-click menu to complete these operations.

   b. The selected configuration node is displayed in the text-exiting area. You can edit this configuration node by manually entering text.

   c. (Optional) Use the toolbar functionalities to modify the configuration on the CLI-based template editor.

   d. (Optional) To include comments in the Template Editor, enter comments in the following format: **#(<configuration node related to the comment>)<comment>**. For example, **# (snmp community**

a1) comments for node snmp community a1 means that the comment for the snmp community *a1* node in the configuration hierarchy is "*comments for node snmp community a1*".

To create a Quick template by using the form-based template editor:

a. Select the **Basic Setup** link.

   The Basic Setup dialog box is displayed.

b. (Optional) In the **Hostname** field, enter the hostname of the device.

c. (Optional) In the **Domain name** field, enter the domain name of the device.

d. (Optional) In the **Timezone** field, enter the time zone of the device.

e. (Optional) Select the **Allow FTP file transfers** check box if you want to allow FTP file transfers on the device.

f. (Optional) Select the **Allow ssh access** check box if you want to allow access to the device through SSH.

g. (Optional) Select the **Allow telnet login** check box if you want to allow access to the device through Telnet.

h. For NTP Server, click the Add NTP Server icon to add an NTP server to the device.

   The Add dialog box is displayed.

   Enter the following details in this dialog box:

   i. In the **Name** field, enter the name of the NTP server.

   ii. (Optional) In the **Key** field, enter a value for the key.

   iii. (Optional) From the **Version** drop-down list, select the appropriate version.

   iv. (Optional) Select the **Prefer** check box.

   v. Click **Create**.

Use the Edit NTP Server and Delete NTP Server icons to edit and delete the NTP server details respectively.

i. For User Management, click the Add User icon to add users for the device.

The Add dialog box is displayed.

Enter the following details in this dialog box:

i. In the **Name** field, enter the name of the user.

ii. (Optional) Select an appropriate user ID from the **User ID** field.

The minimum value for this field is 100.

iii. (Optional) In the **Full Name** field, enter the full name of the user.

iv. (Optional) In the **Password** field, enter the password for the user.

v. (Optional) In the **Re-enter Password** field, reenter the password for the user.

vi. From the **Login Class** drop-down list, select the appropriate login class for the user.

The available login classes are super-user, operator, read-only, unauthorized, and wheel.

vii. Click **Create**.

Use the Edit User and Delete User icons to edit and delete the details of the user respectively.

j. For DNS Server, click the DNS NTP Server icon to add a DNS server to the device.

The Add dialog box is displayed.

Enter the following details in this dialog box:

i. In the **Name** field, enter the name of the DNS server.

ii. Click **Create**.

Use the Edit DNS Server and Delete DNS Server icons to edit and delete the DNS server details respectively.

k. Enter the following SNMP details:

   i. In the **Location** field, enter the location for SNMP.

   ii. Click the Add SNMP Community icon.

   The Add dialog box is displayed.

   For Community, enter the following details:

   a. In the **Name** field, enter the name of the SNMP community.

   b. (Optional) From the **Authorization** drop-down list, select the appropriate type of authorization.

   c. Click **Create**.

   Use the Edit SNMP Community and Delete SNMP Community icons to edit and delete the SNMP Community details respectively.

   iii. Click the Add Trap Group icon.

   The Add dialog box is displayed.

   For Trap Group, enter the following details:

   a. In the **Name** field, enter the name of the trap group.

   b. (Optional) Select the check box next to the appropriate trap group category.

   c. Click **Create**.

   Use the Edit Trap Group and Delete Trap Group icons to edit and delete the trap group details respectively.

l. Click **OK**.

NOTE: If you have installed the Security Director application on your Junos Space Network Management Platform setup and are creating a Quick template by choosing J Series, SRX Series, or LN Series as the device family, you can use the additional Configuration Guides available on the Create Quick Template page. In this case, the Create Quick Template page lists the Configuration Guides to set up routing and security parameters for the Quick template. For more information about using the Configuration Guides related to routing and security parameters for the Quick template, see the *Junos Space Security Director Application Guide*.

> **NOTE:** The Basic Setup Configuration Guide is available only when ACX Series, J Series, M Series, MX Series, T Series, TX Series, PTX Series, EX9200, EX Series, J Series, SRX Series, LN Series, QF Series, or QFX Series is selected as the device family.

8. When you have configured all configuration options required for the Quick template, click **OK**.

9. (Optional) Click the **Variable Settings** button on the lower left to configure the order of the variables and the default value for these variables.

   The Variable Settings page is displayed. You can view all the variables you want to use in the configuration in the Variables area on the left of the page and view the Variable Settings area on the right of the page.

   To configure variable settings:

   a. To reorder variables, use the up and down arrows in the Variables area.

   b. (Optional) In the **Display Name** field, enter a user-defined display name.

   c. (Optional) In the **Default Value** field, enter the default value of the variable.

   d. (Optional) In the **Valid RegEx** field, enter a regular expression.

   e. (Optional) You can either save these variable settings and revisit them later or download to your computer in CSV format.

      - To download the variables and their settings in CSV format, click the **Generate CSV Format** button.
      - To save the variables and their settings without downloading, click the **Save** button.

10. (Optional) Preview the configuration before saving it by clicking the **Preview** button.

11. You can save the Quick template for future modifications or immediately deploy the Quick template to devices.

    - To save the Quick template, click **Save**.

      You are redirected to the Templates page.

    - To deploy the Quick template, click **Save and Assign/Deploy**.

      You are redirected to the Deploy Template page.

NOTE:

- To erase specific configuration from a device by using a Quick template, replace the SET commands with DELETE commands by using the CLI-based Template editor and deploy the Quick template to the device.

  Such templates are also known as negative templates.

- If you undeploy a negative template from a device, the configuration that you removed during the deployment is reset.

For more information about deploying a Quick template, see "Deploying a Quick Template" on page 515.

RELATED DOCUMENTATION

Device Templates Overview | 462

Creating a Device Template | 494

Deploying a Quick Template

You deploy a Quick template to update the configuration on the devices. Before deploying a Quick template to a device, ensure that you have not assigned the template to the same device. If you assign a Quick template to a device and use the Deploy workflow to deploy that Quick template on the same device, although the Quick template is deployed to the device, Junos Space Network Management Platform does not reflect this managed status. The managed status of the device is shown as "Space Changed" on the Device Management page.

You can also use this workflow to assign and publish the Quick template to the devices. You assign and publish a template to the devices to set up this template for deployment. When you assign and publish a Quick template to the devices, the Quick template is placed in queue. You can review the accumulated configuration changes that will be deployed to the devices.

To deploy or assign a Quick template to the devices:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

   The Templates page is displayed.

2. Select the Quick template that you want to deploy and select **Assign/Deploy Template** from the Actions menu.

The Assign/Deploy Template page that appears displays the devices on which the template can be deployed.

3. From the **Selected Template Version** drop-down list, select the version of the device template that you want to deploy or assign to the devices.

4. You can deploy the Quick template by selecting the devices manually, by filtering devices by the device properties, by using tags, or by providing a CSV file with filter criteria:
   - To manually deploy a Quick template, enter the search criteria in the Search field and click the Search icon.

     The list of devices are filtered by the search criteria.
   - To filter devices by device properties, select the check box next to the appropriate device column on the **Column Filter** drop-down list.
   - To select a device by using tags, select an appropriate tag from the **Tag Filter** drop-down list.
   - To provide filter criteria through a CSV file, click the CSV Filter icon and upload the CSV file with the filter criteria by using the Upload a CSV pop-up window.
5. Click **Next**.

   The Resolve Variables page is displayed. This page displays the devices you selected, their managed status, validation status, and the validity of the variable.

6. (Optional) You can resolve the device-specific values in the Quick template either manually or by using a CSV file that specifies device-specific values.

   To resolve device-specific values manually:

   a. From the Resolve Device Specific Value drop-down list, select **Manual**.

   b. Select the devices on which you want to resolve the values from the left of the page.

c. Click the **Template Parameters** tab on the right of the page.

- Enter the device-specific value and click the Add icon.

  If you entered a valid value, the Variable column on the left displays PASS. If you entered an invalid value, the Variable column displays FAIL.

> **NOTE:** You can also enter different values by selecting a device and entering the device-specific value.

d. To view the XML and CLI formats of the configuration that will be deployed, click the **Change Summary** tab.

- Click the **XML** or **CLI** tab.

e. Click the **Validate on Device** link to validate the configuration.

   By validating the configuration, you ensure that the Quick template is semantically correct. If the validation fails, change the template parameters appropriately.

To resolve device-specific values using a CSV file:

a. From the Resolve Device Specific Value drop-down list, select **From a CSV**.

b. Select the devices on which you want to resolve the values from the left of the page.

c. Click **Browse** and select the CSV file from the right of the page.

d. Click **Upload**.

e. (Optional) If you have uploaded a CSV file with filter criteria earlier, select the CSV file from the **Select a csv to apply on chosen devices** drop-down list.

f. Click **Apply CSV**.

g. To view the XML and CLI formats of the configuration that will be deployed, click the **Change Summary** tab.

- Click the **XML** or **CLI** tab.

h. Click the **Validate on Device** link to validate the configuration.

By validating the configuration, you ensure that the Quick template is semantically correct. If the validation fails, change the template parameters appropriately.

7. (Optional) To go back and select more devices or a different set of devices, click **Back**.

   You are directed to the Resolve Variables page.

8. Click **Next**.

9. Select whether to deploy the Quick template now or later or whether to only assign and publish it.

   - To assign and publish the Quick template, select the **Assign and Publish to pending configuration changes** option button.
   - To deploy the Quick template now, select the **Deploy Now** option button.
   - To deploy the Quick template later:

     a. Select the **Deploy Later** option button.

     b. Enter the date in the **Date** field in the DD/MM/YYYY format.

     c. Enter the time in the **Time** field in the hh:mm format.

   NOTE: If you publish the Quick template, the configuration in the Quick template is deployed to the device along with the candidate configuration for the device, with the Junos OS confirmed-commit functionality.

10. Click **Finish**.

    The Deploy Template Job Information dialog box is displayed. You are redirected to the Templates page.

11. Click **OK** to close the dialog box.

    The Quick template is deployed to devices.

    NOTE: If you select modeled devices that are in the Modeled state, the Deploy Now and Deploy Later buttons are disabled.

RELATED DOCUMENTATION

Device Templates Overview | 462
Creating a Quick Template | 509

CHAPTER 29

Device Template Administration

IN THIS CHAPTER

- Viewing Template Details | 520
- Viewing the Device-Template Association (Device Templates) | 521
- Viewing Template Definition Statistics | 524
- Viewing Device Template Statistics | 525
- Comparing Templates or Template Versions | 525
- Comparing a Device Template Configuration with a Device Configuration | 527
- Cloning a Template in Junos Space Network Management Platform | 529
- Exporting and Importing a Quick Template in Junos Space Network Management Platform | 530
- Deleting Device Templates from Junos Space Network Management Platform | 532

Viewing Template Details

You view the details of a template to determine the device template configuration. You can view the template configuration in XML and CLI formats.

> **NOTE:** You cannot view device-specific values in the template configuration by using this workflow.

To view the details of a template:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

   The Templates page that appears displays all the device templates that currently exist in the Junos Space Platform database.

2. Select the template for which you want to view details and select **View Template Details** from the toolbar.

The Template Details page is displayed. You can view the name of the template, versions of the template, and Junos OS version used in the template. You can also view the XML and CLI formats of the template configuration.

3. (Optional) To select the version of the template, select the version from the **Selected Template Version** drop-down list.

4. To select the appropriate view of the configuration:
   - Click the **CLI** tab to view the CLI configuration.
   - Click the **XML** view to view the XML configuration.

Click **Cancel**.

You are redirected to the Templates page.

RELATED DOCUMENTATION

Creating a Device Template | 494
Modifying a Device Template | 502

Viewing the Device-Template Association (Device Templates)

You view the device-template association to determine the version of the template that is deployed or assigned to devices, and the audit status of the template for each deployment.

To view the device-template association:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

   The Templates page is displayed.

2. Right-click the template and select **View Template Association**.

   The View Template Association page is displayed. Table 53 shows the columns on this page.

   Table 53: View Template Association Page

Column Header	Description
Name	Name of the devices to which the template is deployed

Table 53: View Template Association Page *(continued)*

Column Header	Description
Device Alias	Value of the Device Alias custom label for the device. This field is empty if the Device Alias custom label is not added or no value is assigned to the Device Alias custom label for the device.
Domain	Domain to which the template is assigned
IP Address	IP address of the devices to which the template is deployed
Deployed Version	Version of the template that is deployed to the device
Assigned Version	Version of the template that is assigned to the device
Latest Version	Latest version of the template
Deploy Time	Time at which the template was deployed to the device
Deployed By	Username of the user who deployed the template to the device
Job ID	ID of the deployment job
Audit Status	Audit status of the template
Audit Time	Time at which the template was audited

3. You can perform the following tasks on this page:

- To view the details of the device to which the template is assigned or deployed:
  i. Double-click the corresponding device name or IP address column.

     The Device Details dialog box is displayed. You can view the details of the device.

  ii. Click **Close** to close the pop-up window.

- To view the configuration in the template that is deployed to the device:
  i. Click the number in the Deployed Version column.

     The Template Change Summary pop-up window is displayed. You can view the configuration that was deployed to the device.

ii. Click **Close** to close the pop-up window.

- To view the configuration in the template that is assigned to the device:

  i. Click the number in the Assigned Version column.

  The Template Change Summary pop-up window is displayed. You can view the configuration in the template that is assigned to the device.

  ii. Click **Close** to close the pop-up window.

- To view the status of the template deployment job:

  i. Click the job ID in the Job Id column.

  The Job Management page is displayed. You can view the results of the template deployment job.

  ii. Close the Job Management page.

  iii. Repeat steps 1 and 2 to navigate to the View Template Association page.

- To view the audit status of the template:

  i. Click the link in the Audit Status column.

  The Template Audit Result pop-up window is displayed.

  Under the Audit Status heading, any differences found last time the template was audited are listed. Such differences will be due to someone having altered the device configuration between the two template deployments.

  > **NOTE:** To view any differences between a template and the configuration on the devices to which it has been deployed, first ensure an audit has been performed on the template since it was deployed. For more information about auditing a template, see "Auditing a Device Template Configuration" on page 505.

- To export the results of the audit status:

  i. Click the **Export Audit** button.

  ii. Click **Save** to save the results of the audit status in XML format.

4. To return to the Templates page from the View Template Association page, click **Cancel**.

RELATED DOCUMENTATION

Device Templates Overview | 462
Auditing a Device Template Configuration | 505

Viewing Template Definition Statistics

You can view the template definition statistics when you select the Device Templates workspace. The Template Definition Status pie chart presented on the Device Templates page display the states of the template definitions. The chart is interactive. The Template Definition Status pie chart shows published and unpublished template definitions (available for template creation and unavailable, respectively).

To view the template definition statistics:

1. On the Junos Space Network Management Platform user interface, select **Device Templates** .

   The Device Templates page is displayed. This page displays the charts related to device templates and template definitions.

2. Click a specific label on the Template Definition Status chart, for example, click the **Published** label.

   You will be redirected to the Definitions page that is filtered based on the label you clicked.

   To save the pie chart as an image or to print for presentations or reporting, right-click the pie chart and use the menu to save or print the image.

RELATED DOCUMENTATION

Device Templates Overview | 462
Viewing Device Template Statistics | 525

Viewing Device Template Statistics

You can view the device template statistics when you select the Device Templates workspace. The charts presented on the Device Templates page display the states of the device templates and the number of device templates per device family. All the charts are interactive.

The Device Templates page displays the following charts related to device templates:

- Template Status—this pie chart shows the device templates that are enabled, disabled, and needing review. The device templates based on a template definition that is currently in a published state are enabled. The device templates based on a template definition that is currently unpublished are disabled. The device templates based on a republished template definition are marked as needing review.
- Template Count by Device Family—this bar chart shows the number of device templates per device family (each device template can apply to only one device family).

To view the device template statistics:

1. On the Junos Space Network Management Platform user interface, select **Device Templates** .

   The Device Templates landing page is displayed. This page displays the charts related to device templates and template definitions.

2. Click a specific label on the Template Status chart for example, click the **Needs Review** label.

   You will be redirected to the Templates page that is filtered based on the label you clicked.

   To save a chart as an image or to print for presentations or reporting, right-click the chart and use the menu to save or print the image.

RELATED DOCUMENTATION

Device Templates Overview | 462
Viewing Template Definition Statistics | 524

Comparing Templates or Template Versions

You compare two templates or two versions of the same template to view the differences between the configurations that they push to devices.

To compare two templates or two versions of the same template:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

   The Device Templates page that appears displays the list of templates that currently exist in the Junos Space Platform database.

2. Select the templates that you want to compare and select **Compare Template Versions** from the Actions menu.

   The Compare Template Versions page that appears displays versions of templates you want to compare.

3. (Optional) To select a pair of templates for comparison:
   a. From the **Source Template** drop-down list, select the version of the source template.
   b. From the **Template File Version** drop-down list, select the version of the source template.
   c. From the **Target Template** drop-down list, select the target template.
   d. From the **Template File Version** drop-down list, select the version of the target template.
4. Click **Compare**.

   The Compare Template Versions page is displayed.

   You can view the differences between the configurations that are pushed to the devices by these templates. The configuration from the source template is displayed on the left and the configuration from the target template is displayed on the right.

5. (Optional)To view the differences between the templates one by one, use the **Prev Diff** and **Next Diff** buttons on the top-right corner.

Click **Close** to return to the Compare Template Versions page. Alternatively, click **Cancel** to return to the Templates page.

RELATED DOCUMENTATION

Creating a Device Template | 494

Modifying a Device Template | 502

Comparing a Device Template Configuration with a Device Configuration | 527

Comparing a Device Template Configuration with a Device Configuration

You compare the configuration in a device template with the configuration in a device to view the differences between the configurations. To compare the device template configuration with the device configuration, the configurations must belong to the same device family.

To compare a device template configuration with a device configuration:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

   The Templates page that appears displays all the templates that currently exist in the Junos Space Platform database.

2. Select the device template that you want to compare with and select **Compare Template Against Device** from the Actions menu.

   The Compare Template Against Device page is displayed. You can view the name of the template, current selected version of the template, Junos OS version of the template, and a list of all managed devices that belong to the same device family. The **Include All Managed Devices** check box is selected by default. Clear this selection to list only those devices that are UP and in INSYNC states.

3. (Optional) From the **Selected Template Version** drop-down list, select the version of the template.

4. You can search for devices to compare with manually by using columns that represent the status of the device, by using tags, or by providing a CSV file with filter criteria.

   - To search for devices manually, enter the search criteria in the Search field and click the Search icon.

     The list of devices is filtered by the search criteria.

   - To filter devices by device properties, select the check box next to the appropriate device on the **Column Filter** drop-down list.
   - To select devices by using tags, select an appropriate tag from the **Tag Filter** drop-down list.
   - From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.

     To provide filter criteria through a CSV file, click the CSV Filter icon and upload the CSV file with the filter criteria by using the Upload a CSV pop-up window.

5. Click **Next**.

   The devices that you selected are listed on the left of the page.

6. Select whether to compare the template configuration against the configuration in the devices immediately or later:

- To compare the template configuration against the configuration in the devices now, click **Finish**.
- To schedule this task for a later time:
  a. Select the **Schedule at a later time** option button.
  b. Enter the date in the **Date** field in DD/MM/YYYY format.
  c. Enter the time in the **Time** field in hh:mm format.

7. (Optional) Click the **Recurrence** check box and specify the frequency at which to compare the device template configuration against the device configuration.

8. Click **Finish**.

   The Compare Config Job Information page is displayed. To view details of the comparison job, click the job ID. You are redirected to the Job Management page with a filtered view of the job. Double-click the row corresponding to the job to view the detailed status of the job on the Compare Config Job Status page. For devices that are OUTOFSYNC or DOWN, the summary of the job displays a warning message.

   To export the report of comparison, click **Export** button. You are prompted to save the file. Click **OK** on the File Save page to save the file.

   The details of the comparison job, along with the warning message, is listed in the exported report.

Click **OK** to close the page.

Release History Table

Release	Description
17.2	From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.

RELATED DOCUMENTATION

Creating a Device Template | 494
Modifying a Device Template | 502

Cloning a Template in Junos Space Network Management Platform

You clone a template when you want to create a copy of an existing template. You can clone Quick templates and Configuration templates by using this workflow. If you clone a template with multiple versions, only the latest version is cloned.

When you clone a template, a new template is added to the Junos Space Network Management Platform database. This template is assigned the Create state and the version number is set to 1.

To clone a template in Junos Space Platform:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

   The Templates page that appears displays the list of templates that currently exist in the Junos Space Platform database.

2. Select the template that you want to clone and select **Clone Template** from the Actions menu.

   The Clone Template Confirmation dialog box is displayed.

3. In the **Name** field, enter the name of the template.

   A default name for the cloned template is displayed. You can modify this name. The name cannot begin or end with a special character and can contain at most 63 characters.

4. (Optional) In the **Description** field, enter a description of the template.

   The description is optional and limited to 255 characters.

5. Click **OK**.

   A new template is created. You are redirected to the Templates page.

RELATED DOCUMENTATION

Creating a Device Template | 494

Modifying a Device Template | 502

Comparing a Device Template Configuration with a Device Configuration | 527

Exporting and Importing a Quick Template in Junos Space Network Management Platform

IN THIS SECTION

- Exporting a Quick Template | 530
- Importing a Quick Template | 531

You export a Quick template to save it to a local machine. You import a Quick template to import it to the Junos Space Network Management Platform database.

Quick templates are exported and imported in XML format. Perform the following tasks to export and import Quick templates to and from Junos Space Platform.

Exporting a Quick Template

To export a Quick template:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

   The Templates page that appears displays a list of templates that currently exist in the Junos Space Platform database.

2. Select the Quick template that you want to export and select **Export Quick Template** from the Actions menu.

   The Export Quick Template dialog box is displayed.

3. Click the **Download file for the latest version of selected template in XML format** link.

   A dialog box is displayed.

4. Click **OK** to save the XML file to the local machine.

Click **Close** to return to the Templates page.

Importing a Quick Template

To import a Quick template:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

   The Templates page that appears displays the list of templates that currently exist in the Junos Space Platform database.

2. Click the Import Quick Template icon on the toolbar.

   The Import Quick Template dialog box is displayed.

3. Click Browse and select the Quick template XML file.

4. Click **Import**.

   A progress bar indicates the progress of the import job.

   If a Quick template with the same name exists in the Junos Space Platform database, a new page is displayed with an alternative name for the Quick template.

5. (Optional) Double-click the **New Mapped Name** column on the page and modify the name of the Quick template.

6. Click **Import**.

   A progress bar is displayed.

   If you provided a unique name, the Quick template is imported. You can view this Quick template on the Templates page.

You are redirected to the Templates page.

RELATED DOCUMENTATION

Quick Templates Overview | 508

Creating a Quick Template | 509

Deploying a Quick Template | 515

Deleting Device Templates from Junos Space Network Management Platform

You delete templates from Junos Space Network Management Platform when you do not want to use these templates to push configurations to the devices. You can delete templates and their associated versions if they are in the Created state.

> **NOTE:** You can delete multiple versions of a template by using this workflow. However, you cannot delete a version of a template if it is assigned or deployed to the devices.

To delete templates from Junos Space Platform:

1. On the Junos Space Network Management Platform user interface, select **Device Templates > Templates**.

   The Templates page that appears displays the list of templates that currently exist in the Junos Space Platform database.

2. Select the templates that you want to delete and click the Delete Template icon on the toolbar.

   The Delete Template pop-up windowis displayed. You can view the details of the templates and their versions. The state of the template and the date when the template was last modified are displayed.

3. Select the versions of the templates that you want to delete and click **Delete**.

   The versions of the templates that are either assigned or deployed to the devices are not available for selection.

   The selected versions of the templates are deleted. You are redirected to the Templates page.

> **NOTE:** If you delete a device template that is scheduled to be deployed or assigned to the devices, the scheduled job fails.

RELATED DOCUMENTATION

Creating a Device Template | 494

Modifying a Device Template | 502

Comparing a Device Template Configuration with a Device Configuration | 527

4

PART

CLI Configlets

Overview | **534**

CLI Configlets | **548**

Configuration Views | **581**

XPath and Regular Expressions | **600**

Configuration Filters | **605**

CHAPTER 30

Overview

IN THIS CHAPTER

- CLI Configlets Overview | 534
- CLI Configlets Workflow | 537
- Configlet Context | 541
- Nesting Parameters | 546

CLI Configlets Overview

IN THIS SECTION

- Configlet Variables | 535
- Velocity Templates | 536
- Directives | 536

CLI Configlets are configuration tools provided by Junos OS that enable you to easily apply a configuration to a device. CLI Configlets contain the Junos OS configuration as formatted ASCII text. Junos Space uses the NETCONF protocol to load and commit the configuration on to devices.

A CLI Configlet is a configuration template that is transformed into a CLI configuration string before being applied to a device. The dynamic elements (strings) in the configuration template are defined using template variables. These variables act as input to the process of transformation to construct a CLI configuration string. These variables can contain the interface name, device name, description text, or any such dynamic values. The value of these variables are obtained from the user or system or given by the context at the time of execution. Velocity templates (VTL) are used to define CLI Configlets.

You can access the CLI Configlets workspace by selecting CLI Configlets from the left pane. From the CLI Configlets workspace, you can perform the following tasks:

- View the details and statistics of CLI Configlets in Junos Space Network Management Platform.
- Create, modify, clone, or delete a CLI Configlet.
- Apply a CLI Configlet to the devices or submit the configuration changes from a CLI Configlet to the change requests that are deployed using the Review/Deploy Configuration workflow from the Devices workspace. Configuration changes for CLI Configlets created for grouped execution are displayed as change requests for the devices to which the CLI Configlets are submitted.
- Mark and unmark CLI Configlets as favorites.
- Export CLI Configlets from Junos Space Platform.
- Import CLI Configlets from a local computer in the XML format. Starting with Junos Space Network Management Platform Release 15.2R1, you can also import CLI Configlets from a local computer in the TAR (containing XML files) format and from an external Git repository. For more information about Git repository management on Junos Space Platform, see "Git Repositories in Junos Space Overview" on page 1485.

You can also apply CLI Configlets to devices from the Devices workspace. It can be triggered from the actual elements for which the configuration has to be applied. The context of the element for which the CLI Configlet is being applied is called an execution context.

NOTE: CLI Configlets are not supported on SSG Series devices, NetScreen Series devices, TCA Series devices, BXOS Series devices, and Junos Content Encore devices.

Configlet Variables

Variables in CLI Configlets include a leading "$"character. CLI Configlets use three kinds of variables: default, user-defined, and predefined.

Default Variables

The value of these variables need not be input by the user; these values are derived from the current execution context. Table 54 lists the default variables.

Table 54: Default Variables

Variable	Value
$DEVICE	Name of the host on which the CLI Configlet is applied
$INTERFACE	Name of the interface for which the CLI Configlet is applied
$UNIT	Unit number of the logical interface for which the CLI Configlet is being applied

Table 54: Default Variables *(continued)*

Variable	Value
$CONTEXT	Context of the element for which the CLI Configlet is applied

User-Defined Variables

The values for these variables are entered by the user at execution time. Text fields or selection fields are used to obtain data from the user.

Predefined Variables

These are the variables for which the values are predefined when you create the CLI Configlet. These variables are also called invisible parameters because they cannot be modified by the user.

Velocity Templates

Junos Space Network Management Platform enables you to define the device configuration in the form of velocity templates (VTL). These templates are called CLI Configlets. The VTL variable is a reference type, which includes the leading "$" character, followed by a VTL Identifier. CLI Configlets are transformed into a CLI configuration string before they are applied to the device. This transformation is directed by references and directives of VTL.

References are used to embed dynamic contents in the configuration text. Directives allow dynamic manipulation of the contents.

Refer to http://velocity.apache.org/engine/1.7/user-guide.html for detailed information about VTL.

Directives

Directives include an included CLI Configlet's contents and parameters in the base CLI Configlet and import the metadata information related to the parameters of the included CLI Configlet. You can include CLI Configlets in Junos Space Network Management Platform by using two directives: #include_configlet and #mixin directives.

#include_configlet – This directive includes an included CLI Configlet's contents and parameters in the base CLI Configlet and imports the metadata information related to the parameters of the included CLI Configlet. If you define a new parameter in the base CLI Configlet by using the #include_configlet directive, the metadata information is fetched and used from the included CLI Configlets. The parameter values updated in the included CLI Configlet after their inclusion into the base CLI Configlet are not updated and available for the base CLI Configlet. If both the base CLI Configlet and included CLI Configlet contain parameters with a common name, the metadata information related to the parameters is ignored.

#mixin – This directive differentiates the parameters of the base CLI Configlet from the parameters of the included CLI Configlet on the Junos Space user interface. The parameter values for the included CLI

Configlets can be modified even when you apply the CLI Configlet to the device. You cannot include CLI Configlets that have a period (.) or space in its name.

You include these directives in the base CLI Configlet in the following format:

- **#include_configlet("<name of the included configlet>")**
- **#mixin("<name of the included configlet>")**

Release History Table

Release	Description
15.2R1	Starting with Junos Space Network Management Platform Release 15.2R1, you can also import CLI Configlets from a local computer in the TAR (containing XML files) format and from an external Git repository.

RELATED DOCUMENTATION

CLI Configlets Workflow | 537

Creating a CLI Configlet | 548

Modifying a CLI Configlet | 552

Viewing CLI Configlet Statistics | 552

CLI Configlets Workflow

A CLI Configlet can be defined from the CLI Configlets workspace. Table 55 lists the parameters to be defined for a CLI Configlet.

Table 55: Parameters for a CLI Configlet

Parameter	Description
Name	Name of the CLI Configlet. The name cannot exceed 255 characters. Allowable characters include the hyphen (-), underscore (_), letters, and numbers and the period (.). You cannot have two configlets with the same name.
Category	Category of the CLI Configlet. The category cannot exceed 255 characters. Allowable characters include the hyphen (-), underscore (_), letters, and numbers and the period (.).

Table 55: Parameters for a CLI Configlet *(continued)*

Parameter	Description
Device Family Series	Device family series for which the CLI Configlet is applicable.
Context	Context for which the CLI Configlet is applicable. This is an optional field.
Description	Description of the CLI Configlet. The description cannot exceed 2500 characters. This is an optional field.
Preview options	Selecting the Show Parameters option displays the parameters that are present in the CLI Configlet. The Show Configuration option displays the consolidated configuration before the CLI Configlet is applied.
Post-view options	Selecting the Show Parameters option displays the parameters that are present in the CLI Configlet. The Show Configuration option displays the consolidated configuration after the CLI Configlet is applied.
Configlet Content	The actual CLI Configlet is defined here. The CLI Configlet can contain multiple pages and follows a tablike structure. The configuration being applied onto the device can be split among multiple pages. When the configuration is applied, all the pages are combined in order of the page numbers and applied onto the device in a single commit operation. You must always validate the CLI Configlet before moving to the next page.
Reference Number	The range of values are from 1 to 2^{16}.

NOTE: You cannot move to the next page if the contents of the CLI Configlet are invalid. Validation includes bracket matching.

Parameters are variables defined in the CLI Configlet whose values are either retrieved from the environment or entered by the user during execution. When the user applies CLI Configlets, the user is asked to input values for all variables defined in the CLI Configlet.

To configure a parameter, click the modify icon on the toolbar. The Edit Configlet Parameter page is displayed. Use this page to set the attributes of a parameter.

To add an additional parameter, click the add icon on the toolbar. The Add Configlet Parameter page is displayed. The attributes of a parameter are set from this page.

To delete a parameter, click the delete icon on the toolbar. By default, all variables present in the CLI Configlet are listed on the Parameters page. Local variables must be deleted manually or set to the “Invisible” type.

Table 56 lists the attributes of the CLI Configlet parameters.

Table 56: Attributes of CLI Configlet Parameters

CLI Configlet Parameter Attributes	Description
Parameter	Name of the parameter If displayed with a name space in the *<configlet name>.<parameter.name>* format, this parameter belongs to the included CLI Configlet.
Display Name	Display name of the parameter
Description	Description of the parameter
Types	The types of parameters supported are: • **Text field** – You can provide a custom value when executing the CLI Configlet. The default value for this field can be configured with an XPath in the Configured Value Xpath field or with a plain string in the Default Value field. This returns a single value. • **Selection field** – You can select a value from a set of options when executing this CLI Configlet. The default value for this field can be configured with an XPath in the Configured Value Xpath field or with a plain string in the Default Value field. The options can be configured by an XPath in the Selection Values Xpath field, or by using a CSV string in the Selection Values field. This returns a single value. **NOTE:** Though this returns a single value, the return value is of the array type and the selected value can be taken from index 0. • **Invisible field** – You cannot edit this field. This parameter refers to values defined explicitly as a CSV string in the Default Value field or by an XPath in the Configured Value Xpath field. This field returns an array of values. • **Password field** – You need to enter a value when you apply a CLI Configlet containing the parameter. This hides sensitive information in the Apply CLI Configlet job results. • **Password Confirm field** – You need to enter a value twice when you apply a CLI Configlet containing the parameter. This hides sensitive information in the Apply CLI Configlet job results.

Table 56: Attributes of CLI Configlet Parameters *(continued)*

CLI Configlet Parameter Attributes	Description
Configured Value XPath	This field is used to give the XPath of the configured values. The behavior of this field depends on the type of parameter. When the parameter type is a text field or selection field, the corresponding value present in the XPath is taken as the default value. This value can be modified. If the XPath returns multiple values, the first value returned is considered. When the parameter type is an invisible field, the list of values returned by the XPath is taken as the value of the parameter. Invisible field has configured value XPath and selection value XPath only when the parameter scope is either device specific or entity specific. This is disabled if the scope is global. **NOTE:** When using $INTERFACE, $UNIT, Configured Value Xpath field, Invisible field, and Selection field, the variable definition in the Configlet Editor should contain **.get(0)** in order to fetch the value from the array. For example, $INTERFACE.get(0).
Default Value	Displays the same behavior as the Configured Value Xpath field except that the value is given explicitly. This field is considered only when configured value XPath is not specified or if the XPath does not return any value.
Selection Values XPath	This field is enabled only if the parameter type is a Selection field. This field contains the XPath (with reference to the device XML) to fetch the set of values for the Selection field.
Selection Values	This field is the same as the Selection Values XPath field except that the value is given explicitly. This field is considered only when selection values XPath is not specified or if the XPath does not return any value. **NOTE:** Comma-separated values can be used to provide an array of values in the Default Value and Selection Values fields. **NOTE:** While defining the XPath, you must directly access the text node with the **text ()** function. Otherwise the complete XML path of the node is returned. For example, **/device/interface-information/physical-interface/name/text()** to fetch the names of all interfaces.
Order	Order of the parameter. This is the relative order in which the field must be displayed for user input at the time of execution.

Table 56: Attributes of CLI Configlet Parameters *(continued)*

CLI Configlet Parameter Attributes	Description
Regex Value	This field contains regular expression for the parameter that is used to validate the parameter value while you apply the CLI Configlet to the device.
Read-only	Whether the parameter belongs to the base configlet or the included configlet: • false – This parameter belongs to the base configlet. • true – This parameter belongs to the included configlet. The parameter cannot be modified or deleted from this configlet.

RELATED DOCUMENTATION

CLI Configlets Overview | 534

Creating a CLI Configlet | 548

Viewing CLI Configlet Statistics | 552

Configlet Context

Execution of scripts and CLI configlets may be required in some case. For example, one might need to restrict the scope of execution of 'disable interface' script to just the interfaces that are enabled. Having a context associated to the script or configlet solves this problem of restricting the scope. Context of an element is basically a unique path which leads to its XML counterpart in the device XML.

For all context related computations, we consolidate the XMLs fetched form the device under one node called device. This includes configuration XML, interface-information XML, chassis-inventory XML, and system-information XML.

An example of a device XML is as follows:

```
<device>
 <interface-information>.....</interface-information>
 <system-information>.....</system-information>
 <chassis-inventory>.....</chassis-inventory>
 <configuration>....</configuration>
```

```
 ....
</device>
```

Table 57 shows the commands to view the XML from the CLI of the device.

Table 57: Commands to View XML from the CLI

XML type	Command
Chassis Inventory	> show chassis hardware | display xml
Interface Information	> show interfaces | display xml
Configuration	> show configuration | display xml
System Information	-

NOTE: The command for system information XML is not available. An instance of the system information XML is as follows:

```
<system-information>
<hardware-model>ex4200-24t</hardware-model>
<os-name>junos-ex</os-name>
<os-version>11.3R2.4</os-version>
<serial-number>ABCDE12345</serial-number>
<host-name>ex-device1</host-name>
<virtual-chassis/>
</system-information>
```

Context of an Element

There is a need to have the ability to restrict a script or configlet execution to certain elements of interest. For example, one might need to restrict the scope of execution of 'disable interface' script only to the interfaces that are enabled. Having a context associated with the script or configlet solves this scoping problem.

The context of an element is the XPath that maps to the XML node that represents the element in the device XML. Table 58 lists the type of element, XML referred, and the content path.

Table 58: Context Path and XML node referred for different element types

Element Type	XML Referred	Context Path
Device	N/A	/device
Physical Inventory element	Chassis Inventory	/device/chassis-inventory/*
Physical Interface	Interface Information	/device/interface-information/*
Logical Interface	Configuration	/device/configuration/*

Table 59 lists some examples for XPaths for different elements.

Table 59: XPaths for different elements

Element	Context	Description
Device	/device	The context of a device
Chassis	/device/chassis-inventory/chassis[name='Chassis']	Context of a chassis
Routing Engine	/device/chassis-inventory/chassis[name='Chassis']/chassis-module[name='Routing Engine 0']	The context of a routing engine
FPC	/device/chassis-inventory/chassis[name='Chassis']/chassis-module[name='FPC 1']	The context of an FPC in slot 1
PIC	/device/chassis-inventory/chassis[name='Chassis']/chassis-module[name='FPC 1']/chassis-sub-module[name='PIC 4']	The context of a PIC in slot 4 under FPC in slot 1
Logical Interfaces	device/configuration/interfaces/interface[name='ge-0/0/1]/unit[name='0']	The context of logical interface ge-0/0/1.0
Physical Interfaces	/device/interface-information/physical-interface[name='ge-0/1/1]	The context of a physical interface ge-0/1/1

Context filtering

The context attribute of the script or configlet dictates which elements(inventory component or logical interface or physical interface) it is applicable to.

The rule to check whether the script or configlet is applicable to an element is as follows:

- Evaluate the context XPath associated to a script or configlet on the device XML. This results in a set of XML nodes.
- If the resultant XML node list contains the XML node representing the subject element, then the script/template entity is considered a match.

Given below are few examples of script or configlet contexts with their descriptions:

- /device/chassis-inventory/chassis[name='Chassis']/chassis-module[starts-with(name,'Routing Engine')] - Applicable to all routing engines
- /device/chassis-inventory/chassis[name='Chassis']/chassis-module[starts-with(name,'FPC')] - Applicable to all FPCs
- /device[starts-with(system-information/os-version,"11")]/interface-information/ physical-interface[starts-with(name,"ge")] - Applicable to all interfaces of type 'ge' which has system os-version as 11
- /device/interface-information/physical-interface[admin-status=”up”] - Applicable to all physical interfaces with admin status in up state.
- /device/chassis-inventory/chassis[name='Chassis']/chassis-module

  [starts-with(name,'FPC')]/chassis-sub-module[starts-with(name,'PIC')] | /

  device/chassis-inventory/chassis[name='Chassis']/chassis-module

  [starts-with(name,'FPC')]/chassis-sub-module[starts-with(name,'MIC')]

  /chassis-sub-sub-module[starts-with(name,'PIC')] - Applicable to all PICs

> **NOTE:** If we intend to specify the scope of a script as PICs, then we would have to consider two different XPaths the PIC can take (One with MIC in-between and one without). We have to give an OR combination of both the XPaths.

NOTE:

- If no context is associated to a script or configlet, then the context of the script is taken as /device. These scripts or configlets would be listed for execution in devices.
- You can execute CLI Configlets on more than 200 devices only if the CLI Configlets do not require XPath processing. CLI Configlets that do not require XPath processing include CLI Configlets without device-specific or entity-specific parameters and with /, //, or /device as context.

Physical Interface Example

Consider the following device XML

```
<device>
 <interface-information>
  <physical-interface>
   <name>ge-0/0/0</name>
   <admin-status>up</admin-status>
    ....
  </physical-interface>
  <physical-interface>
   <name>ge-0/0/1</name>
   <admin-status>down</admin-status>
    ....
  </physical-interface>
  .....
 </interface-information>
 ....
 <!-- ALL THE OTHER NODES -->
 ....
</device>
```

Context of an element

Context of physical-interface ge-0/0/0 is /device/interface-information/physical-interface[name='ge-0/0/0']

This XPath maps to the node below. This is the XML counterpart of the interface ge-0/0/0

```
<physical-interface>
 <name>ge-0/0/0</name>
 <admin-status>up</admin-status>
  ....
```

```
</physical-interface>
```

Physical Interface in “up” state:

If the user wants to write a configlet to set the admin status of an interface down if its up, the context of the script can be set as /device/interface-information/physical-interface[admin-status='up']

This configlet will be enabled only for interfaces with admin status up. Since in our example, ge-0/0/0 satisfies the above condition, this configlet can be executed on it.

RELATED DOCUMENTATION

- CLI Configlets Overview | 534
- CLI Configlets Workflow | 537
- Creating a CLI Configlet | 548

Nesting Parameters

You can use XPath context to define the default option or selectable options of a parameter. This XPath could have dependencies on other parameters. Consider the example below A configlet requires two inputs, a Physical Interface (Input-1) and a Logical Interface (Input-2) that is a part of the selected Physical Interface(Input-1). We define a parameter PHYINT to get the name of the physical interface and a parameter LOGINT to get the name of the logical interface. We define the SELECTIONVALUESXPATH for PHYINT as "/device/interface-information/physical-interface/name/text()". User selects a value from the options listed by the XPath. Since the selection values listed for LOGINT parameter is dependent on the value selected for PHYINT, we can define the SELECTIONVALUESXPATH of LOGINT as "/device/configuration/interfaces/interface[name='$PHYINT']/unit/name/text()". This ensures that, only the logical interfaces of the selected physical interface are listed.

A configlet could refer another configlet present in Junos Space Network Management Platform using the following statement:

```
#include_configlet("<CONFIGLET-NAME>")
```

Junos Space Network Management Platform would merge the referred configlets inline.

Create a configlet named 'SayHello'

```
#set( $person = "Bob" )
Hello $person
```

Create another configlet named 'Greeting'

```
This is a greeting example
#include_configlet("SayHello")
```

When the confilget 'Greeting' gets evaluated, it generates the following string.

```
This is a greeting example
Hello Bob
```

RELATED DOCUMENTATION

- CLI Configlets Overview | 534
- Configlet Context | 541
- Creating a CLI Configlet | 548

CHAPTER 31

CLI Configlets

IN THIS CHAPTER

- Creating a CLI Configlet | 548
- Modifying a CLI Configlet | 552
- Viewing CLI Configlet Statistics | 552
- Viewing a CLI Configlet | 553
- Exporting CLI Configlets | 556
- CLI Configlet Examples | 557
- Deleting CLI configlets | 565
- Cloning a CLI Configlet | 566
- Importing CLI Configlets | 567
- Applying a CLI Configlet to Devices | 573
- Comparing CLI Configet Versions | 577
- Marking and Unmarking CLI Configlets as Favorite | 578

Creating a CLI Configlet

You create a CLI Configlet to push a configuration to devices. You can also add parameters to a CLI Configlet. Parameters are the variables defined in the CLI Configlet whose values are either obtained from the environment or given by the user during execution.

To create a CLI Configlet:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configlets.**

   The Configlets page is displayed.

2. Click the Create CLI Configlet icon on the toolbar.

   The Create CLI Configlet page is displayed.

3. In the Name field, enter a name for the CLI Configlet.

The name cannot exceed 255 characters. Allowable characters include the hyphen (-), underscore (_), letters, numbers, and the period (.). You cannot have two CLI Configlets with the same name.

4. In the Category field, enter a name for the category of the CLI Configlet.

   The name of the category cannot exceed 255 characters. Allowable characters include the hyphen (-), underscore (_), letters, numbers, and the period (.).

5. From the **Device Family Series** drop-down list, select the device family for the CLI Configlet.

6. (Optional) From the **Context** drop-down list, select the appropriate context for the CLI Configlet.

7. In the Reference Number field, enter a reference number for the CLI Configlet.

   The range is 1 through $2^{16}-1$.

8. (Optional) In the Description field, enter a description.

   The description cannot exceed 2500 characters.

9. For Execution Type, select the type of execution.

   The option buttons available are **Single Execution** and **Grouped Execution**.

   By default, the **Single Execution** option button is selected.

   - If you select **Single Execution**, you can apply the CLI Configlet only to one device at a time.
   - If you select **Grouped Execution**, you can apply the CLI Configlet to multiple devices at a time.

10. For Preview options, select the check boxes if you want to view the parameters and the configuration in the CLI Configlet before applying the configuration to devices.

    The check boxes available are **Show Parameters** and **Show Configuration**. By default, both check boxes are selected.

11. For Postview options, select the check boxes if you want to view the parameters and the configuration in the CLI Configlet in the Apply CLI Configlet job results.

    The check boxes available are **Show Parameters** and **Show Configuration**. By default, both check boxes are selected.

12. In the Configlet Editor area, enter the configuration for the CLI Configlet. You can type or manually paste the configuration in the Configlet Editor.

NOTE: You cannot create a CLI Configlet if you do not enter the configuration in the Configlet Editor.

NOTE: You can also create a CLI Configlet to erase specific configuration from the devices. To do so, include the **delete:** statement above the hierarchy level that should be deleted from the devices. When you apply the CLI Configlet to a device, the physical interface of a device, the logical interface of a device, or the physical inventory element of a device, the configuration at the hierarchy level is erased from the device.

For more information about the protocol and syntax used for creating, modifying, and deleting the configuration by using CLI Configlets, see the Junos XML Management Protocol Guide.

NOTE: When you define a configuration of the CLI Configlet, you should specify variables that accept special characters as input within double quotation marks.

13. Click **Next**.

    You can add the parameters for the CLI Configlet on this page.

14. To add a parameter to the CLI Configlet:

    a. Click the Add Parameter icon.

       The Add Configlet Parameter pop-up window is displayed.

    b. In the Parameter field, enter the name of the parameter.

       The name of the parameter cannot exceed 255 characters. Allowable characters include the hyphen (-), underscore (_), letters, numbers, and the period (.).

    c. In the Display Name field, enter a display name for the parameter.

       The display name cannot exceed 255 characters. Allowable characters include the hyphen (-), underscore (_), letters, numbers, and the period (.).

    d. In the Description field, enter a description for the parameter.

    e. From the **Parameter Scope** drop-down list, select an appropriate scope for the parameter.

       The options available are Global, Device Specific, and Entity Specific.

    f. From the **Parameter Type** drop-down list, select an appropriate type of parameter. The options available are:

- Text Field – You can enter any value.
- Selection Field – You can select a value from a set of options.
- Invisible Field – The field displays a value that is explicitly defined by the user or an XPath.
- Password Field – Enter a password to apply the CLI Configlet.
- Password Confirm Field – Enter the password again to confirm the password.

g. From the **Regex Value** drop-down list, select an appropriate regular expression value.

   This field is enabled if you choose the type of parameter as Text Field, Password Field, or Confirm Password Field.

h. From the **Configured Value Xpath** drop-down list, select an appropriate XPath value.

   This field is enabled if you choose the type of parameter as Text Field, Selection Field, or Invisible Field. This is the XPath (with reference to the device XML) to fetch the set of values.

i. In the Default Value field, enter a default value.

   This field is enabled if you choose the type of parameter as Text Field, Selection Field, or Invisible Field. This field is considered only when the XPath is not specified.

j. From the **Selection Values Xpath** drop-down list, select an appropriate XPath value.

   This field is enabled if you choose the type of parameter as Selection Field. This is the XPath (with reference to the device XML) to fetch the set of values.

k. In the Selection Values field, enter an appropriate selection value.

   This field is enabled if you choose the type of parameter as Selection Field.

l. In the Order field, enter the order in which the parameters should be listed while applying the CLI Configlet.

m. Click **Add**.

15. (Optional) Add multiple parameters.

16. (Optional) To go back to the previous page, click **Back**.

    You are redirected to the previous page.

17. Click **Create**.

    The CLI Configlet is created. You are redirected to the Configlets page.

RELATED DOCUMENTATION

CLI Configlets Overview | 534

Applying a CLI Configlet to Devices | 573
Exporting CLI Configlets | 556
Viewing a CLI Configlet | 553

Modifying a CLI Configlet

You modify a CLI configlet when you want to change the properties of the CLI configlet.

To modify a CLI configlet:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configlets.**

   The Configlets page is displayed.

2. Select the CLI configlet you want to modify and select the Modify CLI configlet icon on the Actions menu.

   The Modify CLI configlet page is displayed.

3. Modify the CLI configlet properties and click **Update**.

   The CLI configlet is modified.

RELATED DOCUMENTATION

CLI Configlets Overview | 534
Creating a CLI Configlet | 548
Exporting CLI Configlets | 556
Importing CLI Configlets | 567

Viewing CLI Configlet Statistics

You can view the statistics about the CLI configlets from the CLI Configlets workspace. The CLI Configlets landing page displays the CLI Configlet Count by Device Family bar chart. The bar chart shows the number of CLI Configlets on the y axis and device family series on the x axis.

To view the statistics of CLI configlets:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets**.

The CLI Configlets landing page is displayed. This page displays the charts related to CLI configlets and configuration views.

2. Click a specific label on a chart.

   You will be redirected to the Configlets page that is filtered based on the label you clicked.

   To save the bar chart as an image or to print for presentations or reporting, right-click the bar chart and use the menu to save or print the image.

RELATED DOCUMENTATION

- CLI Configlets Overview | 534
- Creating a CLI Configlet | 548
- Exporting CLI Configlets | 556

Viewing a CLI Configlet

CLI Configlets are created to modify the configuration on devices. You can view the details of a CLI Configlet on the Configlets page and when you select a CLI Configlet to view the details of a CLI Configlet.

To view the details of a CLI Configlet:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configlets**.

   The Configlets page is displayed.

2. Right-click a CLI Configlet and select **View CLI Configlet Details** or double-click a CLI Configlet.

   The View CLI Configlet dialog box is displayed. This dialog box displays additional information that is not displayed on the Configlets page.

   Table 60 lists the columns displayed on the Configlets page and the fields in the View CLI Configlet dialog box.

   Table 60: CLI Configlet Details

Field or Column	Description	Location
Name	Name of the CLI Configlet	Configlets page View CLI Configlet dialog box
Domain	Domain to which the CLI Configlet is assigned	Configlets page

Table 60: CLI Configlet Details *(continued)*

Field or Column	Description	Location
Category	Category of the CLI Configlet	Configlets page View CLI Configlet dialog box
Device Family Series	Device family series for which the CLI Configlet is applicable	Configlets page View CLI Configlet dialog box
Latest Version	Latest version of the CLI Configlet	Configlets page
Git Version	Commit ID of the CLI Configlet in the Git repository when the CLI Configlet was last imported to Junos Space Platform from the Git snapshot. N/A is displayed if the CLI Configlet was created and modified in Junos Space Platform. A Warning icon is displayed if the CLI Configlet was modified in Junos Space Platform after being imported from the Git snapshot.	Configlets page
Git Branch	Git branch from which the CLI Configlet was last imported N/A is displayed if the CLI Configlet was created and modified in Junos Space Platform.	Configlets page
Description	Description of the CLI Configlet	Configlets page View CLI Configlet dialog box
Execution Type	Whether the CLI Configlet can be applied to one device or multiple devices: Single or Grouped	Configlets page View CLI Configlet dialog box
Creation Time	Date and time when the CLI Configlet was created	Configlets page
Last Updated Time	Date and time when the CLI Configlet was last modified	Configlets page Displayed as Updated Time in the View CLI Configlet dialog box

Table 60: CLI Configlet Details *(continued)*

Field or Column	Description	Location
Last Modified By	Username of the user who last modified the CLI Configlet	Configlets page Displayed as Modified By in the View CLI Configlet dialog box
Reference Number	Reference number assigned to the CLI Configlet	Configlets page View CLI Configlet dialog box
Context	Context for which the CLI Configlet is applicable	View CLI Configlet dialog box
Preview Show Parameters	Whether to view the parameters of the CLI Configlet before applying the CLI Configlet: Enabled or Disabled	View CLI Configlet dialog box
Preview Show Configuration	Whether to view the configuration in the CLI Configlet before applying the CLI Configlet: Enabled or Disabled	View CLI Configlet dialog box
Postview Show Parameters	Whether to view the parameters of the CLI Configlet after applying the CLI Configlet: Enabled or Disabled	View CLI Configlet dialog box
Postview Show Configuration	Whether to view the configuration in the CLI Configlet after applying the CLI Configlet: Enabled or Disabled	View CLI Configlet dialog box
Configlet Content	Contents of in the CLI Configlet	View CLI Configlet dialog box

3. (Optional) To view the contents of a specific version of a CLI Configlet, select the version from the Configlet Version drop-down list.

   The contents of the selected version of the CLI Configlet are displayed in the Configlet Content field.

4. Click **Close** to close the View CLI Configlet dialog box.

RELATED DOCUMENTATION

CLI Configlets Overview | 534

Creating a CLI Configlet | 548

Applying a CLI Configlet to Devices | 573

Exporting CLI Configlets

You export the CLI configlets when you want to download a copy of the CLI configlets to your local computer.

To export CLI configlets:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configlets.**

   The Configlets page is displayed.

2. You can select and export specific CLI configlets or export all configlets on the Configlets page.
   - To export specific CLI configlets:
     a. Select the CLI configlets and select **Export Selected CLI Configlets** from the Actions menu.

        The Export CLI Configlets pop-up window is displayed.

     b. Click **Export** and save the file on your local computer.
   - To export all CLI configlets:
     a. Select **Export All CLI Configlets** from the Actions menu

        The Export CLI Configlets pop-up window is displayed.

     b. Click **Export** and save the file on your local computer.

   The CLI configlets are exported.

RELATED DOCUMENTATION

CLI Configlets Overview | 534

Creating a CLI Configlet | 548

CLI Configlet Examples

Default Configlets are added during server start up or data migration. These default configlets are added only on the initial server start up and during data migration. The user can perform all the usual operations on the default Xpath and Regex, including delete operation.

Adding default configlets during migration has the following conditions:

- 13.1 to 13.3:
  - Default Configlets are added if an entity with the same name does not exist in 13.1.
  - Default Configlets are over written if an entity with the same name exists in 13.1.
- 13.3 to later releases:
  - Default Configlets are not added or overwritten, if the default Configlet is modified or deleted by the user in 13.3.

Example 1: Setting the description of a physical interface

Context: /device/interface-information/physical-interface This configlet is targeted for physical interface.

Configlet

```
interfaces {
   $INTERFACE{
      description "$DESC";
   }
}
```

Parameters

Parameter	Details
$INTERFACE	This is a default variable and the value would be the name of the interface which the configlet is invoked from. This would be null if the configlet is invoked from CLI Configlets workspace as the execution is not associated to a specific interface.
$DESC	A text field to get the description string. The value is got at the time of execution.

On applying the CLI Configlet, the user needs to input the parameters. For our example, user needs to input a value for $DESC.

Consider our example being applied to an interface ge-0/1/3 and the following values are given as input.

Parameter	Value
$DESC	TEST DESC

The generated configuration string would be

```
interfaces {
   ge-0/1/3{
      description "TEST DESC";
   }
}
```

Example 2: Setting the vlan of a logical interface, where the vlan id is chosen from a predefined set of values

Context: /device/configuration/interfaces/interface/unit This CLI Configlet is targeted for logical interface

CLI Configlet

```
interfaces {
   $INTERFACE {
      vlan-tagging;
      unit $UNIT{
         vlan-id $VLANID.get(0);
      }
   }
}
```

##Since VLAN id will be given as a selection field, the value would be a collection and to get the first selected value, use .get(0)

Parameter	Details
$INTERFACE	This is a default variable and the value would be the name of the interface which the CLI Configlet is invoked from. This would be null if the CLI Configlet is invoked from CLI Configlets workspace as the execution is not associated to a specific interface.
$UNIT	This is a default variable and the value would be the unit name of the logical interface which the CLI Configlet is invoked from. This would be null if the CLI Configlet is invoked from CLI Configlets workspace as the execution is not associated to a specific logical interface.

Parameter	Details
$VLANID	This is a selection field and the value would be chosen at the time of execution. **Type**: Selection Field **Selection Values**: 0,1,2,3 **Default Value**: 3

On applying the CLI Configlet, the user needs to input the parameters. For our example, user needs to input a value for $VLANID.

Consider our example being applied to an interface ge-0/1/3.3 and the following values are given as input.

> **NOTE:** Since $VLANID is defined as a selection field, the user has to select one value form a list. The list of options are either specified by Selection Values Xpath or in Selection Values field. The default selection in the list would be 3 as defined in the default value field.

Parameter	Value
$VLANID	2

The generated configuration string would be

```
interfaces {
   ge-0/1/3 {
      vlan-tagging;
      unit 3{
         vlan-id 2;
      }
   }
}
```

Example 3: Setting a description on all the interfaces of a device

Context: NULL or /device. Targeted to a device, the context of a device can either be null or /device

CLI Configlet

```
interfaces {
```

```
    #foreach($INTERFACENAME in $INTERFACENAMES)
    $INTERFACENAME {
      description "$DESC";
    }
    #end
}
```

Parameter	Details
$INTERFACENAMES	An invisible variable with an XPath configured to fetch all the interface names. **Configured values XPath**: /device/interface-information/physical-interface/name/text()
$DESC	A text field to get the description string. The value is got at the time of execution.

The following input is given while executing the CLI Configlet

Parameter	Value
$DESC	TEST DESC

The generated configuration string would be (when the device has three physical interfaces, ge-0/0/0, ge-0/0/1 and ge-0/0/2).

```
interfaces {
    ge-0/0/0 {
        description "TEST DESC";
    }
    ge-0/0/1 {
        description "TEST DESC";
    }
    ge-0/0/2 {
        description "TEST DESC";
    }
}
```

Example 4: Setting a configuration in all the PICs belonging to a device and certain configuration only on the first PIC of FPC 0

Context: NULL or /device. Targeted to a device, the context of a device can either be null or /device

##$ELEMENTS : /device/chassis-inventory/chassis/chassis-module[starts-with(name,"FPC")]

/name/text() | /device/chassis-inventory/chassis/chassis-module

[starts-with(name,"FPC")]/chassis-sub-module[starts-with(name,"PIC")]/name/text()

##this will contain the list of all FPCs and PICs in Depth-first traversal order.

##Hierarchy array is a 2 dimensional array used to store FPC-PIC hierarchy, with each row containing PICs belonging to a single FPC. The first element is the FPC.

CLI Configlet

```
#set( $HIERARCHY = [] )
#set( $LOCALARRAY = [])
#foreach ( $ELEMENT in $ELEMENTS )
#if($ELEMENT.startsWith("FPC"))
## Create a new array for each FPC with the first element as FPC
#set( $LOCALARRAY = [$ELEMENT])
#set( $result = $HIERARCHY.add($LOCALARRAY))
#elseif($ELEMENT.startsWith("PIC"))
## Add the PIC in the current Local array., This is the array of the parent FPC
#set( $result = $LOCALARRAY.add($ELEMENT))
#end
#end
  chassis {
    redundancy {
      failover on-disk-failure;
      graceful-switchover;
    }
    aggregated-devices {
      ethernet {
        device-count 16;
      }
    }
 #foreach ($HIERARCHYELEMENT in $HIERARCHY )
 $HIERARCHYELEMENT.get(0) {
 #set($HIERARCHYELEMENTSIZE = $HIERARCHYELEMENT.size() - 1)
 #foreach ($HIERARCHYELEMENTINDEX in [1..$HIERARCHYELEMENTSIZE] )
 $HIERARCHYELEMENT.get($HIERARCHYELEMENTINDEX){
```

```
## Set the tunnel services setting for the first PIC in FPC 0
#if($HIERARCHYELEMENTINDEX == 1 && $HIERARCHYELEMENT.get(0) == "FPC 0")
 tunnel-services {
    bandwidth 1g;
    }
    #end
    traffic-manager {
       ingress-shaping-overhead 0;
       egress-shaping-overhead 0;
       mode ingress-and-egress;
    }
    }
    #end
    }
    #end
 }
```

Parameters

Parameter	Details
$ELEMENTS	This is an invisible field and the value cannot be set by the user at the time of execution. The values are taken form a predefined XPath **Type**: Invisible field **Configured Value XPath**: /device/chassis-inventory/chassis/chassis-module[starts-with(name,"FPC")] /name/text()/device/chassis-inventory/chassis/chassis-module[starts-with (name,"FPC")]/chassis-sub-module[starts-with(name,"PIC")]/name/text() This XPath returns the list of FPCs and PIC is Depth First Traversal order.

While executing this CLI Configlet, the XPath of $ELEMENTS param will return the list of FPCs and PIC present in the device. The values for instance would be [FPC 0,PIC 0,PIC 1, FPC 1, PIC 0, PIC 1] This order implies the association

FPC 0

PIC 0

PIC 1

FPC 1

PIC 0

PIC 1

When the CLI Configlet is executed, we get the following configuration string

```
chassis {
    redundancy {
        failover on-disk-failure;
        graceful-switchover;
    }
    aggregated-devices {
        ethernet {
            device-count 16;
        }
    }
    fpc 1 {
        pic 0 {
            tunnel-services {
                bandwidth 1g;
            }
            traffic-manager {
                ingress-shaping-overhead 0;
                egress-shaping-overhead 0;
                mode ingress-and-egress;
            }
        }
        pic 1 {
            traffic-manager {
                ingress-shaping-overhead 0;
                egress-shaping-overhead 0;
                mode ingress-and-egress;
            }
        }
    }
    fpc 2 {
        pic 0 {
            traffic-manager {
                ingress-shaping-overhead 0;
                egress-shaping-overhead 0;
                mode ingress-and-egress;
            }
        }
        pic 1 {
            traffic-manager {
```

```
            ingress-shaping-overhead 0;
            egress-shaping-overhead 0;
            mode ingress-and-egress;
        }
    }
  }
}
```

Example 5: Halting the description of a physical interface

Context: /device/interface-information/physical-interface This CLI Configlet is targeted for physical interface

CLI Configlet

```
interfaces {
  #if( $INTERFACENAME == 'ge-0/0/0')
  #terminate('Should not change description for ge-0/0/0 interfaces.')
  #{else}
  $INTERFACENAME {
    unit 0 {
      description "Similar desc";
      family ethernet-switching;
    }
  }
  #end
}
```

Parameter	Details
$INTERFACENAME	A variable with an XPath configured to fetch all the interface names. **Configured Value XPath**: //device/interface-information/physical-interface/name/text()

NOTE: When using $INTERFACE, $UNIT, Configured Value Xpath, Invisible Params, Selection fields; the variable definition in the configlet editor should contain .get(0) in orderinorder to fetch the value from the array. Eg: $INTERFACE.get(0)

Example 6: Deleting configuration from a physical interface

Context: /device/interface-information/physical-interface This CLI Configlet can be used to delete the configuration enabled on the physical interface to support IEEE 802.3ah link fault management.

CLI Configlet

```
protocols {
    oam {
        ethernet {
            link-fault-management {
                delete: interfaces ge-0/0/0;
            }
        }
    }
}
```

NOTE: Ensure that you insert the **delete:** statement at the proper hierarchy level to avoid necessary configuration being deleted from the device.

RELATED DOCUMENTATION

- CLI Configlets Overview | 534
- Creating a CLI Configlet | 548
- Modifying a CLI Configlet | 552
- Viewing CLI Configlet Statistics | 552

Deleting CLI configlets

You delete CLI configlets when you no longer want to use them to apply configuration to devices.

To delete CLI configlets:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configlets.**

   The Configlets page is displayed.

2. Select the CLI configlets you want to delete and select the Delete CLI Configlets icon from the Actions menu.

   The Delete CLI Configlet pop-up window is displayed.

3. Click **Confirm**.

   The CLI configlets are deleted.

RELATED DOCUMENTATION

- CLI Configlets Overview | 534
- Creating a CLI Configlet | 548
- Exporting CLI Configlets | 556

Cloning a CLI Configlet

You clone a CLI configlet when you want to create a copy of an existing CLI configlet.

To clone a CLI configlet:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configlets.**

   The Configlets page is displayed.

2. Select the CLI configlet you want to clone and select **Clone CLI Configlet** from the Actions menu.

   The Clone CLI Configlet page is displayed. You can modify all the fields of the CLI configlet.

3. Modify the **Name** field.

4. (Optional) Modify the other fields in the CLI configlet and click **Next**.

5. (Optional) Add, modify, or delete the necessary fields.

6. Click **Create**.

   The new CLI configlet is created.

RELATED DOCUMENTATION

CLI Configlets Overview | 534
Creating a CLI Configlet | 548
Exporting CLI Configlets | 556

Importing CLI Configlets

You import CLI Configlets in the XML format to add CLI Configlets from a local computer to the Junos Space Network Management Platform database. You can also import multiple CLI Configlets in a single CLI Configlet XML file. Starting with Junos Space Network Management Platform Release 15.2R1, you can also import CLI Configlets from a Git repository to the Junos Space Network Management Platform database.

NOTE: To select and import multiple CLI Configlet XML files from the local computer:

- Use the Mozilla Firefox or Google Chrome Web browser. Currently, Internet Explorer does not support the selection of multiple files.
- Import multiple XML files in the TAR format.

Using a Git repository to import CLI Configlets creates a snapshot of the CLI Configlet Git repository on Junos Space Platform. You can synchronize CLI Configlets from the Git repository with the snapshot on Junos Space Platform and import CLI Configlets from the Git snapshot even if no active connection exists with the Git repository. For more information about Git repository management on Junos Space Platform, see "Git Repositories in Junos Space Overview" on page 1485.

Junos Space Platform validates the CLI Configlets for the following during import:

- A valid file format. CLI Configlets can be imported in XML format. Starting with Junos Space Network Management Platform Release 15.2R1, CLI Configlets can also be imported in TAR (containing **XML** files) format.
- A valid and unique name

If Junos Space Platform detects a conflict during import and you choose to overwrite the CLI Configlet, the conflicting CLI Configlet is saved with an incremented version number in the domain and all subdomains.

To import a CLI Configlet to Junos Space Platform:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configlets**.

   The Configlets page is displayed.

2. Click the Import CLI Configlet icon on the toolbar.

The Import CLI Configlet page is displayed.

3. Import CLI Configlets from a local computer or the Git snapshot of the CLI Configlet Git repository.

NOTE: The fields on the Junos Space user interface to import CLI Configlets from a Git repository are displayed only if an active Git repository is configured on Junos Space Platform.

a. To import one or more CLI Configlets from the local computer:

   i. Click the **Import from files** option button.

      The Import CLI Configlet page displays the fields to import a CLI Configlet from the local computer.

   ii. From the Import from files expandable area, click **Browse** and select the CLI Configlet file in the XML or TAR format.

   iii. (Optional) To view a sample XML CLI Configlet file, click the **View Sample XML** hyperlink.

      A browser pop-up window is displayed.

      You can download the sample XML file to the local computer.

b. To import one or more CLI Configlets from the Git snapshot:

   i. Click the **Import from git** option button.

      The Import CLI Configlet page displays the fields to import the CLI Configlets from the Git snapshot.

      The Import from git expandable area displays the URL to the active CLI Configlet Git repository and the time when the Git snapshot on Junos Space Platform was last synchronized with the Git repository.

   ii. From the **Git Branch** drop-down list, select the branch on the Git snapshot from which the CLI Configlets should be imported.

      By default, the first branch in the Git snapshot is selected.

   iii. (Optional) To synchronize the Git snapshot on Junos Space Platform with the active CLI Configlet Git repository, click **Sync Now**.

      If the synchronization is successful, the Last Sync field is updated and you can import the latest CLI Configlets.

      By default, the Git snapshot on Junos Space Platform synchronizes with the active CLI Configlet Git repository every hour.

> **NOTE:** If Junos Space Platform cannot connect to the CLI Configlet Git repository, an error message is displayed in a pop-up window. Click **OK** to close the pop-up window.

iv. (Optional) To view a sample XML CLI Configlet file, click the **View Sample XML** hyperlink.

A browser pop-up window is displayed.

You can download the sample XML file to the local computer.

4. Click **Next**.

The Import Configlets page that appears displays the CLI Configlets from the selected Git branch or the local computer, in a table. Table 61 displays the columns in the table.

If you imported CLI Configlets in the TAR format, Junos Space Platform displays the CLI Configlets in the TAR file on the Import Configlets page.

Table 61: Import Configlets page

Column	Description
Configlet	Name of the CLI Configlet
Conflict State	State of the CLI Configlet: NEW, CONFLICT, or NO_CONFLICT The column displays NEW if the CLI Configlet does not exist in Junos Space Platform. If you are importing a CLI Configlet from the Git snapshot, the column displays NO_CONFLICT when the CLI Configlet you are importing was earlier imported from the same branch of the Git snapshot. If you are importing a CLI Configlet from the local computer, the column displays CONFLICT when: • The CLI Configlet with the same name already exists in Junos Space Platform. If you are importing a CLI Configlet from the Git snapshot, the column displays CONFLICT when: • The CLI Configlet was created and modified in Junos Space Platform and is currently imported from the Git snapshot. • The CLI Configlet was earlier imported from the Git snapshot and modified in Junos Space Platform (The Git Version column displays a warning icon). • The CLI Configlet was earlier imported from a different branch of the Git snapshot.
Domain	Domain with which the CLI Configlet is associated The column is empty if the CLI Configlet does not exist in Junos Space Platform.

Table 61: Import Configlets page *(continued)*

Column	Description
Latest Version	Latest version of the identical CLI Configlet that is currently stored in the Junos Space Platform database The column is empty if the CLI Configlet does not exist in Junos Space Platform.
Git Version	Commit ID of the CLI Configlet in the Git repository when the CLI Configlet was last imported to Junos Space Platform from the Git snapshot. • A Warning icon is displayed if the CLI Configlet was modified in Junos Space Platform after importing the CLI Configlet from the Git snapshot. • The column is empty if the CLI Configlet does not exist in Junos Space Platform or if the CLI Configlet was never imported from the Git snapshot.
Git Branch	Git branch from which the CLI Configlet was last imported The column is empty if the CLI Configlet does not exist in Junos Space Platform or if the CLI Configlet was never imported from the Git snapshot.
Last Commit	Commit ID of the last commit operation of the CLI Configlet in the selected branch of the Git repository The column is empty if the CLI Configlet is imported from a local computer.

5. (Optional) To stop importing CLI Configlets that display a CONFLICT state, select the **Exclude conflicting configlets from import** check box.

   All CLI Configlets displaying the Conflict state CONFLICT are removed from the Import Configlets page. The Import Configlets page displays only those CLI Configlets that will be imported to the Junos Space Platform database.

   NOTE: If some CLI Configlets cannot be imported, a warning message is displayed in a pop-up window with the list of CLI Configlets that are not selected for import. Click **OK** to close the pop-up window.

6. Click **Finish**.

> **NOTE:** If you import CLI Configlets displaying the CONFLICT state, a warning message is displayed. Click **OK** to import the CLI Configlets. These CLI Configlets are imported with an incremented version number.

The Import Configlets Job Information dialog box is displayed.

- Click the *Job ID* link to view the job results.

  > **NOTE:** If the fields in the CLI Configlet XML file contains invalid values, the job results display the CLI Configlets that were not imported due to invalid values.

  You are directed to the Job Management page with a filtered view of the job.

- To return to the Configlets page, click **OK**.

When the job is complete, the CLI Configlets are imported to Junos Space Platform.

Release History Table

Release	Description
15.2R1	Starting with Junos Space Network Management Platform Release 15.2R1, you can also import CLI Configlets from a Git repository to the Junos Space Network Management Platform database.
15.2R1	Starting with Junos Space Network Management Platform Release 15.2R1, CLI Configlets can also be imported in TAR (containing **XML** files) format.

RELATED DOCUMENTATION

CLI Configlets Overview | 534

Applying a CLI Configlet to Devices | 573

Exporting CLI Configlets | 556

Applying a CLI Configlet to Devices

You apply a CLI Configlet to devices when you want to push a configuration from the CLI Configlet to the devices. You cannot validate a CLI Configlet or apply a CLI Configlet to more than 200 devices if the CLI Configlet requires XPath processing. However, you can apply CLI Configlets to more than 200 devices if the CLI Configlets do not require XPath processing. CLI Configlets that do not require XPath processing include CLI Configlets with context /, //, or */device* and without device-specific or entity-specific parameters.

> **NOTE:**
> At the time of creating a CLI Configlet:
>
> - If you selected the Single execution type, the CLI Configlet can be applied to only one device.
> - If you selected the Grouped execution type, the CLI Configlet can be applied to multiple devices simultaneously.

To apply a CLI Configlet to devices:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configlets.**

   The Configlets page is displayed.

2. Select the CLI Configlet that you want to apply to the devices and select **Apply CLI Configlet** from the Actions menu.

   The Apply CLI Configlet page is displayed.

3. You can select the devices manually, by using tags, or by providing a CSV file with filter criteria:

   - To select the devices manually, enter the search criteria in the Search field and click the Search icon.

     The list of devices are filtered by the search criteria.

   - To select devices by using tags, select an appropriate tag from the **Tag Filter** drop-down list.
   - From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.

     To provide filter criteria using a CSV file, click the CSV Filter icon and upload the CSV file with the filter criteria through the Upload a CSV pop-up window.

   The Apply CLI Configlet page displays parameters. Only text field and selection field type parameters are displayed.

From Junos Space Platform Release 17.2R1 onward, you can use CSV files to input parameter values when you need to apply configlets on multiple devices. You can upload the parameter values in the specified format as a CSV file.

You can access a sample CSV file by clicking the **Download Configlet Parameters** link. The **SampleParameterCSV**file is downloaded with the parameters already present in an editable grid. Refer to the instructions in the **SampleParametersCSV** file for entering the parameter values. If needed, you can rename the **SampleParameterCSV** file. Add or delete parameters present in the **SampleParametersCSV** file and enter a value for the parameters that you retain in the file. Upload the edited CSV file.

To upload the edited CSV file, click the **Browse** button, select the file, and then click the **Upload** button. The values of parameters in the CSV file are populated to the editable grid. The parameters of CLI Configlet are listed in the grid with pagination support.

4. Double-click the **Value** column for each parameter and enter a value.

   All values are accepted for the text field type parameter. For a selection field type parameter, you should select from one of the values you provided for the parameter. The set of values present and the default value selected were defined when the template was created.

5. (Optional) If you want to apply the CLI Configlet later:

   a. Select the **Schedule at a later time** check box.

   b. Enter the date in the **Date** field in the MM/DD/YYYY or MM/DD/YY format.

   c. Enter the time in the **Time** field in the hh:mm format.

6. Click **Next**.

   The parameter value is validated against the regular expression (if given). If the parameter value violates the regular expression, then a validation error is displayed.

   The Preview area of the Apply CLI Configlet page displays the preview of the CLI Configlet. If you selected to view the parameters and the configuration when previewing the CLI Configlet, the parameters and the configuration are displayed.

The top of the Preview area displays the parameters with the values that are applied to devices. The bottom left of the Preview area displays the devices you have selected. The bottom right of the Preview area displays the configuration that will be applied to the device selected on the left.

- Click on a device to view the configuration that will be applied to the device.

> **NOTE:** The preview options selected in the CLI Configlet determine the contents of the Preview area.

7. Before applying the CLI Configlet, you can validate the configuration in the CLI Configlet on the devices.

   - (Optional) To validate the CLI Configlet on the device, click **Validate**.

     The Validate Results page is displayed.

     A job is triggered. The Progress column displays the progress of validation against each device. When the validation is complete, the results of the validation are displayed. The Status column indicates the results of the validation. If the validation is unsuccessful, the details of the error are displayed on the page.

     > **NOTE:** You can also view the validation results from the Job Management page. To view the validation results, double-click the row corresponding to the job ID and click the **View Results** link corresponding to the device. The Validate CLI Configlet Job Remarks pop-up window is displayed. Navigate back to the Validate Results page.

   - Click **Close**.

     You are redirected to the Apply CLI Configlet page.

8. (Optional) To select a different set of devices or reschedule the workflow, click **Back**.

You are redirected to the previous page.

9. You can apply the CLI Configlet to the devices or submit the configuration changes included in the CLI Configlet to the change requests of the selected devices.

   - i. To apply the CLI Configlet to the device, click **Apply**.

     If you selected to apply the CLI Configlet now, the Configlets Results page is displayed.

     A job is triggered. The Progress column displays the progress of applying the CLI Configlet against each device. When the job is complete, the results of the job are displayed. The Status column indicates the results of the job. If there is an error, the View Job Details page displays an error message. For more information about the error messages, see "Common Error Messages in Device-Related Operations" on page 992.

     > **NOTE:** You can also view the results from the Job Management page. To view the results, double-click the row corresponding to the job ID and click the **View Results** link corresponding to the device. The Apply CLI Configlet Job Remarks pop-up window is displayed. Navigate back to the Configlet Results page.

     ii. If you scheduled this task for a later time, the Job Information page that appears displays the schedule information. Click **OK**.

   - i. To submit the configuration changes to the change requests, click **Submit**.

     The configuration changes are included in the list of changes on the Review/Deploy Configuration page in the Devices workspace.

   An audit log is generated when you apply or submit the CLI Configlet.

- To cancel the task, click **Cancel**. You are returned to the CLI Configlets page.

Release History Table

Release	Description
17.2	From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.
17.2	From Junos Space Platform Release 17.2R1 onward, you can use CSV files to input parameter values when you need to apply configlets on multiple devices.
16.1R1	You can apply the CLI Configlet to the devices or submit the configuration changes included in the CLI Configlet to the change requests of the selected devices.

RELATED DOCUMENTATION

CLI Configlets Overview | 534

Creating a CLI Configlet | 548

Exporting CLI Configlets | 556

Comparing CLI Configet Versions

You compare CLI configlets when you want to view the difference in the configuration it contains. You can compare two different CLI configlets or compare two version of the same CLI configlet.

To compare CLI configlets:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets** > **Configlets**.

   The CLI Configlets page is displayed.

2. Select the CLI configlet that you want to compare and select **Compare CLI Configlet Versions** from the Actions menu.

   The **Compare CLI Configlet Versions** page is displayed.

3. Use the **Source CLI Configlet** and **Target CLI Configlet** lists to select the CLI configlets that you want to compare.

4. Use the **Version** lists to specify the versions of the source and target CLI configlets that you have selected.

5. Click **Compare.**.

   The Compare CLI Configlets window is displayed. This window displays differences between the CLI configlets.

   The differences between the two CLI configlets are represented using three different colors:

   - Green—The green lines represent the changes that appear only in the source CLI configlet.
   - Blue—The blue lines represent the changes that appear only in the target CLI configlet.
   - Purple— The purple lines represent the changes that are different between the two CLI configlets.

   After the **Next Diff** and **Prev Diff** buttons, the total number of differences, the number of differences in the source CLI configlet, the number of differences in the target CLI configlet, and the number of changes are displayed.

6. Use the **Next Diff** and **Prev Diff** buttons to navigate to the next change or the previous change, respectively.

7. Click **Close** to close the window and return to the Compare CLI Configlet Versions page.

RELATED DOCUMENTATION

- CLI Configlets Overview | 534
- Creating a CLI Configlet | 548
- Exporting CLI Configlets | 556

Marking and Unmarking CLI Configlets as Favorite

IN THIS SECTION

- Marking CLI Configlets as Favorite | 579
- Unmarking CLI Configlets Marked as Favorite | 579

To easily identify CLI Configlets that you want to use to push a configuration to a device, mark the CLI Configlets as favorite by using the My Favorite private tag. You can then search for and use the tagged

CLI Configlets in all workflows that support selection by tags. You can unmark the CLI Configlets when you no longer need to identify them.

This topic describes the following tasks:

Marking CLI Configlets as Favorite

To mark CLI Configlets as favorite:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configlets**.

   The Configlets page that appears displays a list of CLI Configlets in the Junos Space Platform database.

2. Select the CLI Configlets that you want to mark as favorite and select **Mark as Favorite** from the Actions menu.

   The Mark as Favorite pop-up window is displayed. The name of the tag is set to My Favorite and the tag is private.

3. (Optional) In the **Description** field, enter a description.

4. Click **Apply Tag**.

   The Mark as Favorite dialog box is displayed.

5. Click **OK**.

   The CLI Configlets are tagged.

   The CLI Configlets that you tagged as favorite are displayed in the Tag view on the CLI Configlets page. You can also view the number of objects that are tagged as My Favorite.

Unmarking CLI Configlets Marked as Favorite

To unmark CLI Configlets marked as favorite:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configlets**.

   The Configlets page that appears displays a list of CLI Configlets that exist in the Junos Space Platform database.

2. Select the CLI Configlets that you want unmark as favorite and select **Unmark as Favorite** from the Actions menu.

   The Unmark as Favorite pop-up window that appears displays that the CLI Configlets are successfully unmarked as favorite.

3. Click **OK**.

   The CLI Configlets are untagged.

RELATED DOCUMENTATION

CLI Configlets Overview | 534

Creating a CLI Configlet | 548

CHAPTER 32

Configuration Views

IN THIS CHAPTER

- Configuration Views Overview | 581
- Configuration View Variables | 582
- Configuration View Workflow | 583
- XML Extensions | 585
- Creating a Configuration View | 586
- Viewing a Configuration View | 588
- Modifying a Configuration View | 589
- Deleting Configuration Views | 590
- Exporting and Importing Configuration Views | 591
- Viewing Configuration Views Statistics | 595
- Default Configuration Views Examples | 595

Configuration Views Overview

Configuration Views are configuration tools provided by Junos OS using which the user can customize how the configuration details are displayed: Form View, Grid View, XML View, or CLI View. Form View offers a simple view of the configuration details as key-value pairs. The dynamic fields in Form View are defined using parameters. Grid View is a customizable grid that shows the key (column) and list of values (rows). The dynamic column values in Grid View are defined using parameter definitions. Velocity templates (VTL) are used to define the parameters. XML and CLI views show the configuration of the selected component in XML and CLI formats respectively.

To access the tasks related to Configuration Views, select **CLI Configlets > Configuration View** from the Junos Space user interface.

You can perform the following tasks:

- Create, modify, or delete Configuration Views.
- View the statistics of the Configuration Views present in Junos Space Network Management Platform.

- Export and import Configuration Views in XML format.

Configuration Views can be generated from the actual elements to which the configuration must be applied. The actual elements are represented in a tree structure of the device configuration in the XML format. The context of the element for which the Configuration View is being created is called the execution context.

RELATED DOCUMENTATION

Creating a Configuration View | 586

Deleting Configuration Views | 590

Default Configuration Views Examples | 595

Configuration View Variables

A parameter name in Configuration View consists of a leading “$”. Configuration View uses three kinds of variables. Configuration views can use the following default variables to define a parameter.

Default Variables

The values of the variables are taken from the current execution context. The following are the default variables.

Variable	Value
$DEVICE	The name of the host which the configuration view is being created
$INTERFACE	Name of the interface for which the configuration view is being created
$UNIT	The unit number of the logical interface for which the configuration view is being created
$CONTEXT	The context of the element for which the configuration view is being created

Velocity Templates

Junos Space Network Management Platform enables the user to define the device configuration view parameter's XPath using Velocity Templates. Nested parameters are referred using VTL. Please refer to http://velocity.apache.org/engine/1.7/user-guide.html for detailed documentation of VTL. VTL variable is a type of reference and consists of a leading "$" character followed by a VTL Identifier.

RELATED DOCUMENTATION

Configuration Views Overview | 581
Creating a Configuration View | 586
Modifying a Configuration View | 589

Configuration View Workflow

A Configuration View can be defined form the CLI Configlets workspace. Table 62 lists the parameters defined for a Configuration View.

Table 62: Parameters defined for a Configuration View

Name	Name of the configuration view. The Name cannot exceed 255 characters. Allowable characters include the dash (-), underscore (_), letters, and numbers and the period (.). You cannot have two configuration views with the same name.
Domain	Domain to which the configuration view is associated
Title	Title of the configuration view. The title cannot exceed 255 characters. Allowable characters include the dash (-), underscore (_), letters, and numbers and the period (.).
Device Family Series	The device family series which the configuration view will be applicable for.
Context	The context for which the configuration view would be applicable for.
Description	Description of the configuration view. The description cannot exceed 2500 characters. This is an optional field.
Order	Order of the configuration view tab in Device Configuration View. The order can accept values from 1 to 65535.
View Type	View types are Form View, Grid View, XML View, and CLI View..

Parameters are the variables defined in the configuration view whose values are got from the environment. Parameters appear when creating or editing a configuration view, as they are added to configuration view. To configure a parameter, click modify icon on the toolbar, the Edit Form View Parameter appears. The attributes of a parameter are set from this screen. To add additional parameter, clicks add icon on the tool bar, the Add Form View Parameter screen appears. The attributes of a parameter are set from this screen. To delete a parameter, click the delete icon on the toolbar. Table 63 lists the attributes of a parameter.

Table 63: Attributes of a parameter

Parameter	Name of the parameter.
Index Parameter	To consider a parameter as an index parameter or not. This is applicable for a grid view only. An index parameter should meet at least one of the following two conditions except when only one parameter is defined in a grid view. • An index parameter should refer at least one of the other index parameters. • An index parameter should be referred in one of the other parameters. A non index parameter should always refer at least one index parameter.
Display Name	Display name of the parameter.
Configured Value XPATH	This field is used to give the XPath of the configured values. The behavior of this field depends on the type of view. When the view type is form, the corresponding value present in the XPath is taken as the field value. In case XPath returns multiple values, first value returned is considered. In case the XPath returns multiple values, the first value returned is considered. When the view type is grid, the following behavior is followed. If more than one parameters defined then following rules should be met. • For independent index parameters, a join would be performed between the values returned by the XPath and the existing set of rows. • For dependent index parameters, join would be performed between the values returned by the XPath and the correspondent row. For non index parameters, if list of values returned then they are aggregated into comma separated values.
Order	The order of the parameter. The relative order in which the parameter has to be displayed.

RELATED DOCUMENTATION

Configuration Views Overview | 581

Creating a Configuration View | 586

Modifying a Configuration View | 589

XML Extensions

In a Configuration View, the querying is not restricted to the Device XML data. Junos Space Platform lets users define parameters that can fetch additional details that are not a part of the device XML itself.

Operational Status

In the config viewer, realtime status of the component could be queried using the XPath <xpath-of-the-component>/oper-status.

> **NOTE:** For physical interface component, <xpath-of-physical-inteface>/oper-status/text() cannot be used. Its only possible to query with <xpath-of-physical-inteface>>/oper-status. This limitation doesn't apply for chassis components.

Customized Attributes

In config viewer, Custom attributes of a component could be queried using the XPath <xpath-of-the-component>/customized-attribute[name='<attribute-name>'].

While defining a view with customized attribute, the user has an option to make it editable. Making a customized attribute editable would allow the user to edit the values inline. Changes would be persisted immediately. To make a customized attribute editable, enable the checkboxes 'Customized Attribute' and 'Editable'. Custom attributes are editable only in Grid View.

> **NOTE:** For custom attributes XPath <xpath-of-the-component>/customized-attribute[name='<attribute-name>'] can be used, but /text() or any other extensions at the end of the XPath cannot be used.

RELATED DOCUMENTATION

- Configuration Views Overview | 581
- Configuration View Variables | 582
- Creating a Configuration View | 586
- Modifying a Configuration View | 589

Creating a Configuration View

You create a configuration view from the Configlets workspace.

To create a configuration view:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configuration View.**

   The Configuration View page is displayed.

2. Click the Create Configuration View icon from the Actions menu.

   The Create Configuration View page is displayed. Table 64 lists the columns displayed on this page.

   Table 64: Columns on the Configuration Views Page

Field	Description
Name	Name of the configuration view
Domain	Domain to which the configuration view is associated
Title	Title of the configuration view
Device Family	Family of the device
Description	Description of the configuration view
Order	Order in which the view has to be applied and it accepts only values greater than zero
View Type	Type of configuration view - Form view, Grid view, XML view, and CLI view
Creation Time	Date and time when the configuration view was created
Last Updated Time	Latest time when the configuration view was last updated
Last Modified By	Login ID of the user who last modified the configuration view

3. In the **Name** field, enter the name for the configuration view

   The Name cannot exceed 255 characters. Allowable characters include the dash (-), underscore (_), letters, and numbers and the period (.). You cannot have two configuration views with the same name.

4. From the **View Type** drop-down list, select the type of configuration view you want to create.

5. In the **Title** filed, enter a title for the configuration view.

   The title cannot exceed 255 characters. Allowable characters include the dash (-), underscore (_), letters, and numbers and the period (.).

6. From the **Device Family Series** drop-down list, select the appropriate device family for which you want to create a configuration filter.

7. From the **Context** drop-down list, select the appropriate XPath value.

8. (Optional) In the **Description** field, enter a description.

   The description cannot exceed 2500 characters.

9. In the **Order** field, enter an appropriate value.

10. Click the Add Parameter icon to add a parameter.

    The Add Form View Parameter pop-up window is displayed. Configure the parameter on this page.

    a. In the **Parameter** field, enter the name of the parameter.

    b. In the **Display Name** field, enter a display name for this parameter.

    c. Select the **Script Dependant** check-box if you want to use a script.

       - If you select the configuration view to depend on a script, select the appropriate local script from the **Local Script** drop-down list.

    d. From the **Configured Value Xpath** drop-down list, select an appropriate XPath value.

    e. In the **Order** field, enter an appropriate value.

    f. Click **Add**.

11. (Optional) Add multiple parameters.

12. Click **Create**.

    The configuration view is created.

> **NOTE:** To assign a configuration view to a domain, select the configuration view and select **Assign Configuration View to Domain** from the Actions menu.

RELATED DOCUMENTATION

Configuration Views Overview | 581

Modifying a Configuration View | 589

Viewing a Configuration View

You view a configuration view when you need to view the details of the configuration view.

To view a configuration view:

1. On the Network Management Platform user interface, select **CLI Configlets > Configuration View**.

   The Configuration View page that appears displays the configuration views.

2. Select the configuration view you want to view and select the **View Configuration View** icon from the Actions bar.

   The View Configuration View dialog box is displayed.

   Table 52 lists the details of the configuration view displayed in the View Configuration View dialog box.

   Table 65: View Template Definition Dialog Box Details

Field or Area	Description	Displayed In
Name	Name of the configuration view	Configuration View page View Configuration View dialog box
Title	Title of the configuration view	Configuration View page View Configuration View dialog box
Device Family	Device family to which the configuration view belongs	Configuration View page
OS Version	Context of the configuration view	Configuration View page View Configuration View dialog box
Description	Description of the configuration view	Configuration View page View Configuration View dialog box

Table 65: View Template Definition Dialog Box Details *(continued)*

Field or Area	Description	Displayed In
Order	Order of the configuration view	Configuration View page View Configuration View dialog box
View Type	Type of the configuration view: Form view, CLI view, Grid view, or XML view	Configuration View page View Configuration View dialog box
Updated Time	Time when the configuration view was last updated	Configuration View page View Configuration View dialog box
Modified By	Username of the user who modified the configuration view	Configuration View page View Configuration View dialog box

3. Click **Close** to close the View Configuration View dialog box.

RELATED DOCUMENTATION

Modifying a Configuration View | 589

Deleting Configuration Views | 590

Creating a Configuration View | 586

Configuration Views Overview | 581

Modifying a Configuration View

You modify a configuration view when you want to change the properties of the configuration view.

To modify a configuration view:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configuration View.**

   The Configuration View page is displayed.

2. Select the configuration view you want to modify and select the Modify Configuration View icon on the Actions menu.

   The Modify Configuration View page is displayed.

3. Modify the properties of the configuration view and click **Update**.

   The configuration view is modified.

RELATED DOCUMENTATION

Configuration Views Overview | 581
Creating a Configuration View | 586

Deleting Configuration Views

You delete configurations view when want to remove it from Junos Space Network Management Platform.

To delete configuration views:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configuration View.**

   The Configuration View page is displayed.

2. Select the configurations views you want to delete and select the Delete Configuration View icon from the Actions menu.

   The Delete Configuration View pop-up window is displayed.

3. Click **Delete**.

   The configuration views are deleted.

RELATED DOCUMENTATION

Configuration Views Overview | 581
Creating a Configuration View | 586

Exporting and Importing Configuration Views

IN THIS SECTION

- Exporting Configuration Views | 592
- Importing Configuration Views | 593

You export Configuration Views from the Junos Space Network Management Platform database to your local computer so that copies of Configuration Views are locally available. Configuration Views are exported in the XML format. You import Configuration Views from your local computer to the Junos Space Platform database so that copies of Configuration Views are stored in the database. Configuration Views are imported in the XML format. You can also overwrite existing Configuration Views in the Junos Space Platform database. An audit log entry is created when you export or import a Configuration View.

> **NOTE:** You cannot export the default Configuration View *Default View* from the Junos Space Platform database. If you select the Default View, the Export Configuration Views option is unavailable.

When you export multiple Configuration Views from Junos Space Platform, they are exported as a single XML file in the following format:

<configuration-views>

<configuration-view>configuration-view1</configuration-view>

<configuration-view>configuration-view2</configuration-view>

<configuration-view>configuration-view3</configuration-view>

<configuration-views>

Exporting Configuration Views

You export Configuration Views in the XML format to your local computer.

To export Configuration Views:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configuration View.**

   The Configuration View page that appears displays all the Configuration Views in the Junos Space Platform database.

2. Select the Configuration Views that you want to export and select **Export Configuration Views** from the Actions menu.

   The Export Configuration Views dialog box is displayed.

3. You can export only those Configuration Views you selected or all Configuration Views (except Default View) from the Junos Space Platform database.

   > **NOTE:** If the Configuration View you selected is script dependent, the local script-name field displays only the name of that local script that is referred to in the Configuration View.

   To export selected Configuration Views:

   a. Click **Export Selected** in the Export Configuration Views dialog box.

      The Export Configuration Views dialog box is displayed. When the job is completed, the Export Configuration Views dialog box indicates that the job is 100% complete.

   b. Click the **Download** link in the dialog box to export the Configuration Views.

      The Configuration Views are downloaded to the local computer.

   To export all Configuration Views:

   a. Click **Export All** on the Export Configuration Views dialog box.

      The Export Configuration Views dialog box is displayed. When the job is completed, the Export Configuration Views dialog box indicates that the job is 100% complete.

   b. Click the **Download** link in the dialog box to export the Configuration Views.

The Configuration Views are downloaded to the local computer.

4. (Optional) Click the progress bar in the Export Configuration Views dialog box to view the details of the job on the Job Management page.

   You are directed to the Job Management page.

To return to the Configuration View page, click the [X] icon in the Export Configuration Views dialog box.

Importing Configuration Views

You cannot import Configuration Views if they contain invalid data such as an invalid script name or an invalid device family. If one of the Configuration Views contain invalid data, the import job fails.

To import Configuration Views:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configuration View.**

   The Configuration View page that appears displays all the Configuration Views in the Junos Space Network Management Platform database.

2. Click the Import Configuration Views icon on the toolbar.

   The Import Configuration Views page is displayed.

3. (Optional) Click the **View Sample Link** on this page to view the valid format of the Configuration View XML file.

4. Click **Browse** and select the Configuration View XML file.

5. Click **Import**.

NOTE: You cannot import Configuration Views if they contain invalid data such as an invalid script name or an invalid device family. If one of the Configuration Views contain invalid data, an error message indicates the reason for the failure of the import job of the Configuration View.

- If the Configuration View you are importing does not exist in the Junos Space Platform database, the Configuration View is imported to the database. When the Configuration View is imported, the Import Configuration Views dialog box is displayed.

  To accept the import of the Configuration View:

  i. Click **OK**.

     You are redirected to the Configuration Views page.

- If a Configuration View with the same name exists in the Junos Space Platform database, the Configuration View Already Exists dialog box is displayed. You can overwrite the existing Configuration View or cancel the workflow.

  - To overwrite an existing Configuration View:

    i. Click **OK**.

       The Import Configuration View dialog box is displayed.

    ii. Click **OK**.

       You are redirected to the Configuration Views page.

  - To avoid overwriting and cancel the workflow:

    i. Click **Cancel**.

       The Import Configuration View dialog box is displayed.

    ii. Click **OK**.

       You are redirected to the Configuration Views page.

RELATED DOCUMENTATION

Configuration Views Overview | 581

Creating a Configuration View | 586

Modifying a Configuration View | 589

Viewing Configuration Views Statistics

You can view the statistics about the configuration views from the CLI Configlets workspace. The Configuration Views landing page displays the Configuration Viewer Count by Device Family bar chart. The bar chart shows the number of configuration views on the y axis and device family series on the x axis.

To view the statistics of configuration views:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets**.

   The CLI Configlets landing page is displayed. This page displays the charts related to CLI configlets and configuration views.

2. Click a specific label on a chart.

   You will be redirected to the Configuration Views page that is filtered based on the label you clicked.

   To save the bar chart as an image or to print for presentations or reporting, right-click the bar chart and use the menu to save or print the image.

RELATED DOCUMENTATION

Configuration Views Overview | 581
Creating a Configuration View | 586
Modifying a Configuration View | 589

Default Configuration Views Examples

Default configuration Views are added during server start up or data migration during an upgrade. These default configuration Views are added only on the initial server start up and data migration during an upgrade. Default configuration Views cannot be added every time the server starts. The user can perform all the usual operations with the default configuration Views including delete operation.

Adding default configuration Views during migration has the following conditions:

- 13.1 to 13.3:

  - Default configuration Views are added if an entity with the same name does not exist in 13.1.
  - Default configuration Views are over written if an entity with the same name exists in 13.1.
- 13.3 to later releases:
  - Default configuration Views are not added or overwritten, if the default configuration Views are modified or deleted by the user in 13.3.

Default view

This view produces the configuration of the selected node in CLI format- curly brace format.

Context: //

This configuration view is targeted for all the entities.

Sample CLI view

Device: EX4200

```
interfaces {
    ge-0/0/4 {
        description "desc";
        unit 0 {
            description "description for Unit;";
        }
    }
}
```

Example XML view

This view produces the configuration of the selected node in XML format.

Context: ///device/configuration/protocols

This configuration view is targeted for protocols.

Sample CLI view

Device: EX4200

```
<!-- Device: Ex4200 -->
<protocols>
    <igmp-snooping>
        <vlan>
```

```
            <name>all</name>
        </vlan>
    </igmp-snooping>
    <rstp>
    </rstp>
    <lldp>
        <interface>
            <name>all</name>
        </interface>
    </lldp>
    <lldp-med>
        <interface>
            <name>all</name>
        </interface>
    </lldp-med>
</protocols>
```

Example Form view

This form view displays certain important information about device.

Context:/device

Sample Form view Details:

Table 66: Parameters

Display name	Script dependent	Parameter	Configured value xpath	Order
Device Name	false	Device_Name	/device/system-information/host-name/text()	1
OS Version	false	OS_Version	/device/system-information/os-version/text()	2
Serial Number	false	Serial_Number	/device/system-information/serial-number/text()	3
Chassis	false	chassis_description	/device/chassis-inventory/chassis/description/text()	4
Location	false	snmp_location	/device/configuration/snmp/location/text()	5
Contact	false	snmp_contact	/device/configuration/snmp/contact/text()	6

Sample Form View:

Device Name: ACX-34

OS Version: 12.3-20130818_att_12q3_x51.0

Serial Number: ABCDE12345

Chassis: ACX1100

Location: location1

Contact: John Doe

Example Grid view

This view displays information about the selected node in Grid format.

Context:/device

Sample Grid View Details

Table 67: Parameters

Parameter	Index parameter	Display name	Script dependent	Customized attribute	Editable	Order
Device_Name	true	Device Name	false	false	false	1
Physical_Interface_Name	true	Physical Interface Name	false	false	false	2
IP_Address	false	IP Address	false	false	false	3
MAC_Address	false	MAC Address	false	false	false	4
Operational_Status	false	OperationalStatus	false	false	false	5
Admin_Status	false	Admin Status	false	false	false	6
Speed	false	Speed	false	false	false	7

Table 68 displays the parameters, configured value Xpaths and the order.

Table 68: Parameters and Configured Value XPath

Parameter	Configured value xpath	Order
Device_Name	`/device/system-information/host-name/text()`	1

Table 68: Parameters and Configured Value XPath *(continued)*

Parameter	Configured value xpath	Order
Physical_Interface_Name	`/device[name='$Device_Name']/interface-information/physical-interface [starts-with(name,'xe')or starts-with(name,'ge-')or starts-with(name,'fe')]/name/ text()`	2
IP_Address	`/device[name='$Device_Name']/configuration/interfaces/interface [name='$Physical_Interface_Name']/unit[name='0'] /family/inet/address/name/text()`	3
MAC_Address	`device[name='$Device_Name']/interface-information/physical-interface [name='$Physical_Interface_Name']/hardware-physical-address`	4
Operational_Status	`/device[name='$Device_Name']/interface-information/physical-interface [name='$Physical_Interface_Name']/oper-status/text()`	5
Admin_Status	`/device[name='$Device_Name']/interface-information/physical-interface [name='$Physical_Interface_Name']/admin-status/text()`	6
Speed	`/device[name='$Device_Name']/interface-information/physical-interface [name='$Physical_Interface_Name']/speed/text()`	7

Sample Grid View

Device Name	Physical interface	IP address	MAC address	Operational status	Admin status	Speed
ACX-34	ge-0/0/0	NA	00:00:5E:00:53:00	down	Up	1000mbps
ACX-34	ge-0/0/1	NA	00:00:5E:00:53:00	down	Up	1000mbps
ACX-34	ge-0/0/2	NA	00:00:5E:00:53:00	down	Up	1000mbps
ACX-34	ge-0/0/3	NA	00:00:5E:00:53:00	down	Up	1000mbps

RELATED DOCUMENTATION

- Configuration Views Overview | 581
- Creating a Configuration View | 586
- Modifying a Configuration View | 589

CHAPTER 33

XPath and Regular Expressions

IN THIS CHAPTER

- XPath and Regex Overview | 600
- Creating Xpath or Regex | 601
- Modifying Xpath and Regex | 601
- Deleting Xpath and Regex | 602
- XPath and Regular Expression Examples | 603

XPath and Regex Overview

While developing configlets, XPaths and Regular Expressions would be used intensively. It would be desirable to let the user define frequently used XPaths and Regular expressions in such a way that they can be referred when required. User can define these templates from the Xpath and Regex task group in the CLI Configlets workspace.

XPaths and Regular expressions defined here are referred from all the fields that require the defined type as input. The user defined values can be selected from the dropdown provided for the field. This can be edited at the field level.

RELATED DOCUMENTATION

Creating Xpath or Regex | 601

Modifying Xpath and Regex | 601

Creating Xpath or Regex

You create Xpath and Regex from the CLI configlets workspace.

To create an Xpath and Regex:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Xpath and Regex.**

   The Xpath and Regex page is displayed.

2. Click the Create Xpath and Regex icon on the Actions menu.

   The Create Xpath/Regex page is displayed.

3. In the **Name** field, enter the name of the Regex or Xpath.

4. From the **Property Type** field, select an appropriate value for the Xpath or Regex.

5. In the **Value** field, enter an appropriate value.

6. Click **Create**.

   The Xpath or regular expression is created.

> **NOTE:** To assign the Xpath or regular expression t a domain, select **Assign Xpath to Domain** from the the Actions menu.

RELATED DOCUMENTATION

- XPath and Regex Overview | **600**
- Modifying Xpath and Regex | **601**
- Deleting Xpath and Regex | **602**

Modifying Xpath and Regex

You modify an Xpath and Regex when you want to change the properties of the Xpath or Regex.

To modify an Xpath and Regex:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Xpath and Regex.**

   The Xpath and Regex page is displayed.

2. Select the Xpath and Regex you want to modify and select the Modify Xpath and Regex icon on the Actions menu.

   The Modify Xpath/Regex page is displayed.

3. Modify the Xpath and Regex properties and click **Update**.

   The Xpath and Regex is modified.

RELATED DOCUMENTATION

XPath and Regex Overview | **600**

Creating Xpath or Regex | **601**

Deleting Xpath and Regex

You delete an Xpath and Regex when you no longer want it on Junos Space Network Management Platform.

To delete an Xpath and Regex:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Xpath and Regex.**

   The Xpath and Regex page is displayed.

2. Select the Xpath and Regex you want to delete and select the Delete Xpath and Regex icon on the Actions menu.

   The Delete Xpath/Regex pop-up window is displayed.

3. Click **Delete**.

   The Xpath and Regex is deleted.

RELATED DOCUMENTATION

XPath and Regex Overview | 600

Creating Xpath or Regex | 601

XPath and Regular Expression Examples

Default Xpath and Regex are added during server start up or data migration performed during an upgrade. These default Xpath and Regex are added only on the initial server start up and during data migration as a result of an upgrade.The User can perform all the usual operations on the default Xpath and Regex, including delete operation.

Adding default Xpath and Regex during migration has the following conditions:

- 13.1 to 13.3:
  - Default Xpath and Regex are added if an entity with the same name does not exist in 13.1.
  - Default Xpath and Regex are over written if an entity with the same name exists in 13.1.
- 13.3 to later releases:
  - Default Xpath and Regex are not added/overwritten, if the default Xpath and Regex is modified/deleted by the user in 13.3.

Example 1 – Alphanumeric

To refer in configlet's Regex Value. It accepts all the alphanumeric characters.

Type: Regular Expression

Value: [a-zA-Z0-9]*

Example 2 - Logical Interfaces per Physical Interface

To fetch the logical interface of selected physical interface

Type: Xpath Context

Value: /device/configuration/interfaces/interface[name="$INTERFACE.get(0)"]/unit/name/text()

Example 3 – Physical Interfaces

To fetch the name of the physical interface

Type: Xpath Context

Value: /device/interface-information/physical-interface/name/text()

Example 4 – Devices

To fetch the name of the selected device

Type: Xpath Context

Value: /device/name/text()

RELATED DOCUMENTATION

XPath and Regex Overview | **600**

Creating Xpath or Regex | **601**

CHAPTER 34

Configuration Filters

IN THIS CHAPTER

- Creating a Configuration Filter | 605
- Modifying a Configuration Filter | 606
- Deleting Configuration Filters | 607

Creating a Configuration Filter

Configuration Filters restrict the scope of the configuration nodes and options displayed in the View Device Configuration page in the Devices workspace. You can create configuration filters for a specific device family in the CLI Confglets workspace. These configuration filters are available in the device configuration page when you configure the device. You can choose these configuration filters in the left pane on the device configuration page.

> **NOTE:** You can also create a configuration filter from the View Device Configuration page. To create a filter, click the **Create Filter** icon on the left of the page.

To create a configuration filter:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets** > **Configuration Filter**

   The Configuration Filter page that appears displays all the configuration filters in the Junos Space Platform database.

   The configuration filter All is displayed by default.

2. Click the **Create Configuration Filter** icon on the Actions menu.

   The Create Configuration Filter page is displayed. The Device Configuration Schema area is displayed on the left and the Device Configuration Area is displayed on the right.

3. In the Name textbox, enter a name for the configuration filter.

4. Select the appropriate device family from the **Device Family** drop-down list.

5. Select the configuration nodes in the Device Configuration Area and click **Create**.

   The configuration filter is created. You are redirected to the Configuration Filter page.

RELATED DOCUMENTATION

Modifying a Configuration Filter | 606
Deleting Configuration Filters | 607

Modifying a Configuration Filter

You modify a configuration filter when you want to change the properties of the configuration filter.

To modify a configuration filter:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configuration Filter**

   The Configuration Filter page is displayed.

2. Select the configuration filter you want to modify and select the **Modify Configuration Filter** icon on the Actions menu.

   The Modify Configuration Filter page is displayed.

3. Modify the properties of the configuration filter and click **Update**.

   The configuration filter is modified. You are redirected to the Configuration Filter page.

RELATED DOCUMENTATION

Creating a Configuration Filter | 605
Deleting Configuration Filters | 607

Deleting Configuration Filters

You delete configuration filters when you want to remove them from Junos Space Network Management Platform.

To delete a configuration filter:

1. On the Junos Space Network Management Platform user interface, select **CLI Configlets > Configuration Filter**

   The Configuration Filter page is displayed.

2. Select the configuration filters you want to delete and select the **Delete Configuration Filter** icon from the Actions menu.

   The Delete Configuration Filter pop-up window is displayed.

3. Click **Confirm** on the Delete Configuration Filter pop-up window.

   The configuration filters are deleted. You are redirected to the Configuration Filter page.

RELATED DOCUMENTATION

Creating a Configuration Filter | 605

Modifying a Configuration Filter | 606

5

PART

Images and Scripts

Overview | **609**

Managing Device Images | **613**

Managing Scripts | **672**

Managing Operations | **730**

Managing Script Bundles | **749**

CHAPTER 35

Overview

IN THIS CHAPTER

- Device Images and Scripts Overview | 609
- Viewing Statistics for Device Images and Scripts | 610

Device Images and Scripts Overview

In Junos Space Network Management Platform, a device image is a software installation package that enables you to upgrade to or downgrade from one Junos operating system (Junos OS) release to another. Scripts are configuration and diagnostic automation tools provided by Junos OS.

The Images and Scripts workspace in Junos Space Platform enables you to manage these device images and scripts.

You can access the Images and Scripts workspace by clicking **Images and Scripts** on the Junos Space Platform UI.

The Images and Scripts workspace enables you to perform the following tasks:

- Manage device images.

  You can upload device images and Junos Continuity software packages from your local file system and deploy them to a device or multiple devices of the same device family simultaneously. After uploading device images and Junos Continuity software packages, you can stage them on a device, verify the checksum, and deploy them whenever required. You can also schedule the staging, deployment, and validation of device images and Junos Continuity software packages.

- Manage scripts.

  You can import multiple scripts into the Junos Space server and perform various tasks such as modifying the scripts, viewing their details, exporting their content, comparing them, and staging them on multiple devices simultaneously. After you stage scripts onto devices, you can use Junos Space Platform to enable, disable, or execute the scripts on those devices.

- Manage operations.

You can create, manage, export, import, and execute operations that combine multiple scripts and image tasks, such as upgrading images and staging or executing scripts, into a single operation for efficient use and reuse.

- Manage script bundles.

  You can group multiple scripts into a script bundle. Script bundles can be staged and executed on devices. You can also modify and delete script bundles.

Junos Space Platform allows you to access and perform tasks in a workspace only if you are assigned the appropriate role or granted the appropriate permissions required for performing that task. Junos Space Platform has a set of predefined user roles that can be assigned to a user to enable access to the various workspaces. For more information about the predefined roles in Junos Space Platform, see "Predefined Roles Overview" on page 999. A User Administrator can also create and assign roles to users from the Role Based Access Control workspace in Junos Space Platform.

RELATED DOCUMENTATION

Device Images Overview | 613

Operations Overview | 730

Scripts Overview | 673

Script Bundles Overview | 749

Viewing Statistics for Device Images and Scripts

In the Images and Scripts workspace, you can view charts that give you an overview of the device images and scripts in Junos Space Network Management Platform. The Images and Scripts statistics page appears when you select Images and Scripts on the task tree of the Junos Space Platform UI. You can view the following bar charts on the Images and Scripts statistics page:

- **Device Image Count by Platform Group**
- **Device Images Count by Version**
- **Number of Scripts by Type**
- **Number of Jobs per Script Action**

To view the **Device Image Count by Platform Group** bar chart:

1. On the Junos Space Platform UI, select **Images and Scripts**.

   The Images and Scripts statistics page appears, displaying the **Device Image Count by Platform Group** bar chart. The x-axis represents the platform and the y-axis represents the number of device images.

Mouse over a platform bar on the Device Image Count by Platform Group chart to view a tooltip showing the number of device images that support the selected platform.

2. (Optional) Click a platform bar on the Device Image Count by Platform Group chart. The Images page appears, displaying the device images in Junos Space Platform that support the selected platform. You can double-click any device image to view its details.

To view the **Device Images Count by Version** bar chart:

1. On the Junos Space Platform UI, select **Images and Scripts**.

   The Images and Scripts statistics page appears, displaying the **Device Images Count by Version** bar chart. The x-axis represents the device image version and the y-axis represents the number of device images. Mouse over a version bar on the Device Images Count by Version chart to view a tooltip showing the number of device images of that version in Junos Space Platform.

2. (Optional) Click a version bar on the Device Images Count by Version chart.

   The Images page appears, displaying the device images of that particular version. You can double-click any device image to view its details.

To view the **Number of Scripts by Type** bar chart:

1. On the Junos Space Platform UI, select **Images and Scripts**.

   The Images and Scripts statistics page appears, displaying the **Number of Scripts by Type** bar chart. The x-axis represents the script type and the y-axis represents the number of scripts. Mouse over a script type bar on the Number of Scripts by Type chart to view a tooltip showing the number of scripts of that script type in Junos Space Platform.

2. (Optional) Click a script type bar on the Number of Scripts by Type chart.

   The Scripts page appears, displaying the scripts of that particular type. You can double-click any script to view its details.

To view the **Number of Jobs per Script Action** bar chart:

1. On the Junos Space Platform UI, select **Images and Scripts**.

   The Images and Scripts statistics page appears, displaying the **Number of Jobs per Script Action** bar chart. The x-axis represents the actions performed on scripts and the y-axis represents the number of jobs triggered. Mouse over the green area of a bar on the Number of Jobs per Script Action chart to view a tooltip showing the number of successful jobs for that script action. Mouse over the red area of the bar to view a tooltip showing the number of failed jobs for that script action.

2. (Optional) Click a script action bar on the Number of Jobs per Script Action chart.

The Job Management page appears, displaying the jobs triggered by that particular action. You can double-click any job to view its details.

> **NOTE:** When you click the green area of a bar, only successful jobs for that action are listed on the Job Management page. When you click the red area of a bar, only failed jobs for that action are listed on the Job Management page.

RELATED DOCUMENTATION

- Device Images and Scripts Overview | **609**
- Device Images Overview | **613**
- Scripts Overview | **673**

CHAPTER 36

Managing Device Images

IN THIS CHAPTER

- Device Images Overview | 613
- Importing Device Images to Junos Space | 615
- Viewing Device Images | 616
- Modifying Device Image Details | 618
- Staging Device Images | 620
- Staging Satellite Software Packages on Aggregation Devices | 625
- Verifying the Checksum | 630
- Viewing and Deleting MD5 Validation Results | 634
- Deploying Device Images | 637
- Deploying Satellite Software Packages on Aggregation and Satellite Devices | 652
- Viewing Device Image Deployment Results | 657
- Viewing Device Association of Images | 659
- Undeploying JAM Packages from Devices | 661
- Removing Device Images from Devices | 666
- Deleting Device Images | 671

Device Images Overview

In Junos Space, a device image is a software installation package that enables you to upgrade to or downgrade from one Junos operating system (Junos OS) release to another. Junos Space Network Management Platform facilitates the management of device images for devices running Junos OS by enabling you to upload device images from your local file system and deploy them on a device or multiple devices of the same device family simultaneously. You can download device images from https://www.juniper.net/customers/support/ . For more information about downloading device images, see the *Junos OS Installation and Upgrade Guide*.

After you upload a device image, you can stage the device image on a device, verify the checksum, and deploy the staged image whenever required. You can also schedule the staging, deployment, and validation

of a device image. You can modify the platforms supported by the device image and the description of the device image.

The Images and Scripts workspace in Junos Space Platform also enables you to manage Junos Continuity software packages (JAM packages) on the MX240, MX480, MX960, MX2010, and MX2020 Series 3D Universal Edge Routers. The filenames for Junos Continuity software packages are prefixed with **jam-** and are referred to as JAM packages in Junos Space Platform. Junos Continuity software packages are optional software packages that enable the router to support new hardware, such as Modular Port Concentrators (MPCs), without Junos OS being upgraded. You can download and install the Junos Continuity software package that supports the MPCs that you want to deploy, from https://www.juniper.net/support/downloads/?p=continuity#sw. For more information about Junos Continuity software and the platforms and hardware supported, see the Junos Continuity software documentation.

From the Images and Scripts workspace of Junos Space Platform, you can also stage and deploy satellite software packages to Juniper Networks devices functioning as aggregation devices and to the satellite devices connected to those aggregation devices. Satellite software packages have names prefixed with **satellite-** and must be downloaded and imported to Junos Space Platform before you can stage or deploy them. For more information about aggregation devices, satellite devices, and satellite software, refer to the *Junos Fusion* documentation.

For more information about aggregation devices and satellite devices in Junos Space Platform, see "Device Inventory Overview" on page 299.

You can perform the following tasks from the Images page:

- Upload device images onto Junos Space Platform.
- View details of the image uploaded to Junos Space Platform.
- Modify a device image.
- Stage a device image on a device.
- View the devices that are associated with a staged image.
- Verify the checksum.
- View and delete MD5 validation results.
- Deploy a device image.
- View device image deployment results.
- Undeploy a JAM package from a device.
- Remove a staged device image from a device.
- Delete device images from Junos Space Platform.
- Assign a device image to a domain.
- Tag and untag the images, view the images that are tagged, and delete private tags.

On the basis of the roles assigned to your username, Junos Space Platform enables or disables different tasks. For more information about the roles that must be assigned to you so that you can perform tasks on device images, see “Predefined Roles Overview” on page 999.

RELATED DOCUMENTATION

Deploying Device Images | 637

Staging Device Images | 620

Modifying Device Image Details | 618

Importing Device Images to Junos Space | 615

Scripts Overview | 673

Script Bundles Overview | 749

Operations Overview | 730

Importing Device Images to Junos Space

Before you can manage a device image using Junos Space Network Management Platform, you must first download the device image from the Juniper Networks Support webpage. You can download device images from https://www.juniper.net/customers/support/. To make the downloaded device image available in Junos Space Platform, save the file to your computer and then import it into Junos Space Platform.

NOTE: You can import satellite software packages and Junos Continuity software packages to Junos Space Platform by following the procedure for importing device images.

- The filenames of satellite software packages intended for deployment on Juniper Networks devices functioning as aggregation devices are prefixed with **satellite-**. You can download satellite software packages from https://www.juniper.net/support/downloads/?p=fusion#sw.
- The filenames of Junos Continuity software packages are prefixed with **jam-** and are referred to as JAM packages in Junos Space Platform. You can download Junos Continuity software packages from https://www.juniper.net/support/downloads/?p=continuity#sw.

To import device images to Junos Space Platform:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Images**.

   The Images page appears.

2. Click the **Import Image** icon.

   The Import Images dialog box appears.

3. Click **Browse**.

   The File Upload dialog box displays the directories and folders on your local file system.

4. Navigate to the device image file that you want to import and click **Open**.

5. Click **Upload** in the Import Images dialog box.

   The time taken to import the file depends on the size of the device image file and the connection speed between your computer and the Junos Space Platform server. After the file is imported to the Junos Space server, it is listed on the Images page. You can now stage and deploy the device image on one or more devices.

RELATED DOCUMENTATION

- Staging Device Images | 620
- Verifying the Checksum | 630
- Deploying Device Images | 637
- Device Images Overview | 613

Viewing Device Images

The Images and Scripts workspace enables you to view and manage multiple device images in Junos Space Network Management Platform. You can view information about all the device images that are stored in the Junos Space Platform database from the Images page. To view detailed information about a particular device image, you can use the View Device Image Detail option on the Actions menu.

NOTE: You can view information about satellite software packages and Junos Continuity software packages imported to Junos Space Platform in the same way that you view information about device images.

- The filenames for satellite software packages intended for deployment on Juniper Networks devices functioning as aggregation devices are prefixed with **satellite-**. The **Type** field for satellite software images displays the value **satellite**.
- The filenames for Junos Continuity software packages are prefixed with **jam-** and are referred to as JAM packages in Junos Space Platform. The **Type** field for Junos Continuity software packages displays the value **jam**.

To view device images from the Images page:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Images**.

   The Images page appears, displaying the device images that you imported into Junos Space Platform.

   Table 69 describes the fields displayed on the Images page.

   You can use the filter option on the **File Name**, **Domain**, and **Version** drop-down lists to specify the filter criteria. When you apply the filters, the table displays only the device images that match the filter criteria. The **Series** and **Associations** fields do not support the filter option.

2. Select an image and click the **View Device Image Detail** icon, or double-click the image whose details you want to view.

   The **Device Image Details** dialog box appears.

   Table 69 also contains the description of fields in the Device Image Details dialog box.

Table 69: Description of Fields on the Images Page and the Device Image Details Dialog Box

Field	Description	Displayed In
File Name	Name of the device image file For example, jinstall-ex-4200-12.3R4.6-domestic-signed.tgz	**Images** page **Device Image Details** dialog box
Domain	Domain to which the device image belongs By default, the image belongs to the **Global** domain.	**Images** page

Table 69: Description of Fields on the Images Page and the Device Image Details Dialog Box *(continued)*

Field	Description	Displayed In
Version	Version number of the device image For example, 12.3R4.6	**Images** page **Device Image Details** dialog box
Series	Series supported by the device image For example, EX4200	**Images** page
Type	Type of file denoted by the prefix of the image filename For example, **jinstall**, **satellite**, and **jam**	**Images** page **Device Image Details** dialog box
Associations	Associated devices for a device image displayed when you click **View** in the **Associations** column	**Images** page
MD5	32-character hexadecimal number that is computed on the device image file stored on the Junos Space server	**Device Image Details** dialog box
Platforms	Platforms supported by the device image	**Device Image Details** dialog box
Description	Description of the device image	**Device Image Details** dialog box

RELATED DOCUMENTATION

- Device Images Overview | 613
- Importing Device Images to Junos Space | 615
- Device Images and Scripts Overview | 609

Modifying Device Image Details

Junos Space Network Management Platform enables you to add and modify the description of a device image and also to modify the series that the device image supports.

NOTE:

- You cannot modify the device series for a Junos Continuity software package because Junos Continuity software packages are supported only on MX240, MX480, MX960, MX2010, and MX2020 Series 3D Universal Edge Routers. Therefore, the **Modify Device Image** action is not available for Junos Continuity software packages.
- You can modify the details of satellite software packages in Junos Space Platform by following the procedure for modifying the details of device images.

To modify the parameters of a device image:

1. On the Junos Space Network Management Platform UI, select **Images and Scripts** > **Images**.

   The Images page appears.

2. Select the image that you want to modify.

   The selected image is highlighted.

3. Click the **Modify Device Image** icon.

   The Modify Device Image dialog box appears.

4. To modify the series, use the **Series** list and specify the series that the selected device image supports.

   The platforms that are part of the selected series are automatically displayed in the **Platforms** field and cannot be modified.

5. To add or modify the description, you can use a maximum of 256 characters within the **Description** box.

6. Click **Modify**.

   Your changes are saved. These changes can be viewed on the device image detail and summary views.

RELATED DOCUMENTATION

Device Images Overview | **613**

Deploying Device Images | **637**

Deleting Device Images | **671**

Staging Device Images

Junos Space Network Management Platform enables you to stage an image or a Junos Continuity software package (JAM package) on one device or multiple devices of the same device family simultaneously. Staging an image enables you to hold a device image on a device, ready to be deployed when needed. At any given time, you can stage only a single device image. Staging images repeatedly on a device merely replaces the previously staged device image. While staging device images, you can also delete existing device images from the device. After you stage a device image, you can verify the checksum to ensure that the device image is transferred completely.

> **NOTE:** You can stage Junos Continuity software packages on devices by following the procedure for staging device images.

To stage a device image on devices:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Images**.

   The Images page appears.

2. Select the device image and select **Stage Image on Device** from the Actions menu. The Stage Image on Devices page appears. The devices that are listed belong to the device family that supports this image.

   This page displays the following information:

   - **Image name**—Filename of the device image that you have selected for staging
   - **MD5 Value**—32-character hexadecimal number that is computed on the selected device image file, which is stored on the Junos Space server
   - **Device Name**—Name of the discovered device, which is an identifier used for network communication between Junos Space Network Management Platform and the Junos OS device.
   - **Device Alias**—Value of the Device Alias custom label for the device. This field is empty if the Device Alias custom label is not added or no value is assigned to the Device Alias custom label for the device.
   - **Domain**—Domain to which the device is assigned
   - **IP Address**—IP address of the discovered device. For example, 10.1.1.1.
   - **Platform**—Platform of the discovered device. For example, MX480.
   - **Software Version**—Operating system firmware version running on the device. For example, 13.1X49D29.1.
   - **Staged Status**—Indicates whether the selected image is staged on the discovered device. This column displays either **Staged** (if the image is staged) or **Not Staged** (if the image is not yet staged).

- **Deployed Status**—Indicates whether the selected Junos Continuity software package is deployed on the device. This column appears only when you select a Junos Continuity software package to be staged. The column displays either **Deployed** (if the Junos Continuity software package is deployed) or **Undeployed** (if the Junos Continuity software package is not deployed).
- **Checksum Status**—Indicates whether the device image on the Junos Space server and the device is the same. The status can be one of the following:
  - **Valid** when the checksum values of the device image on the Junos Space server and the device match
  - **Invalid** when the checksum values do not match
  - **NA** when the selected image is not staged on the device yet

  You can restage an image whose checksum status is "Invalid" to ensure that you stage the image onto the device correctly, thereby making the checksum status "Valid." You can deploy an image only when the checksum status is "Valid."
- **Last Checksum Time**—Time when the checksum was last verified. For a device on which the selected image is not staged yet, this column displays **NA**.

> **NOTE:** You can verify the checksum for a device image by selecting the **Verify Image on Devices** option from the Actions menu. For more information about how to verify the checksum, see "Verifying the Checksum" on page 630.

You can sort the data displayed in the following columns of the Stage Image on Devices page: **Device Name**, **IP Address**, **Platform**, **Software Version**, **Staged Status**, **Checksum Status**, and **Last Checksum Time**.

You can also filter the list of devices based on the data in the following columns: **Device Name**, **IP Address**, **Platform**, and **Software Version**.

3. Select the device or devices on which you want to stage the device image by using one of the following selection modes—manually, on the basis of tags, or by using a comma-separated values (CSV) file. These options are mutually exclusive. If you select one, the others are disabled.

> **NOTE:** By default, the **Select Device Manually** option is selected and the complete list of devices is displayed.

To select devices manually:

a. Click the **Select Device Manually** option, if it is not selected previously.

b. Select the devices on which you want to stage the device image.

   The Select Devices status bar shows the total number of devices that you selected. The status bar is dynamically updated as you select the devices.

c. (Optional) To select all devices, select the check box in the column header next to Device Name.

To select devices on the basis of tags:

a. Click the **Select by Tags** option. The Select by tags list is activated.

b. Click the arrow on the **Select by Tags** list. A list of tags defined for devices in Junos Space Platform appears, categorized into two—Public and Private.

> **NOTE:** If no tags are displayed, then it means that none of the devices is associated with any tag. You must first tag the devices on the Device Management page before you can use the **Select by Tags** option.

c. To select tags, perform one of the following actions :

   - Select the check boxes next to the tag names to select the desired tags and click **OK**.
   - To search for a specific tag, enter the first few letters of the tag name in the **Select by Tags** field to the left of the **OK** button. If a match is found, a suggestion is made. Select the suggested match and click **OK**.

   As you select the tags, the total number of devices associated with the selected tags appears just above the device display table. For example, if there are six devices associated with the selected tags, then **6 items selected** is displayed.

The selected tags appear next to the **Tags Selected** label. An [X] icon appears after each tag name. You can click the [X] icon to clear any tag from the list. The device count decrements accordingly.

From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.

> **NOTE:** By default, the **Include All Managed Devices** check box is not selected. Selecting the check box lists all device managed by Junos Space Platform.

To select devices by using a CSV file:

a. Select the **Select by CSV** option.

b. Click **Browse** and select the file in CSV format containing the list of devices on which you want to stage the device image.

> **TIP:** For a sample CSV file, click the **Sample CSV** link. You are prompted to save the file. Save the file to your local system and open it by using an application, such as Microsoft Excel.

c. Click **Upload** to upload the CSV file.

4. (Optional) To remove existing device images from the device, expand the **Staging Options** section and select the **Delete any existing image before download** check box.

   When you delete a previously staged image, an audit log entry is automatically generated.

5. (Optional) To schedule a time for staging the device image, select the **Schedule at a later time** check box and use the calendar icon and drop-down list, to specify the date and time respectively.

6. Click **Stage Image**.

   The image is staged on the selected device or devices and an alert appears, displaying the job ID. However, if the device on which you are trying to stage the device image does not have sufficient disk space to accommodate the image, then Junos Space displays an error message and the staging job fails.

> **NOTE:** The time taken to stage an image depends on the size of the image, network connectivity, and the number of devices on which the image is staged. You can monitor the progress of the staging job by viewing the **Percent** column of the particular job on the Job Management page. If Junos Space Platform detects an SSH fingerprint mismatch between that on the device and that in the Junos Space Platform database, the connection is dropped. The Connection Status displays Down and Authentication Status displays Fingerprint Conflict on the Device Management page. The View Job Details page displays an error message.

To verify whether the image is staged successfully, click the ***job ID*** link or navigate to the Job Management page and view the status of the job. If the job is a failure, you can double-click the row corresponding to the job to view the reason for failure. The Device Image Action Details page appears, which displays the reason for failure in the **Description** column. If there is an error, the View Job Details page displays an error message. For more information about the error messages, see "Common Error Messages in Device-Related Operations" on page 992. However, if the image is staged successfully, then this column displays a success message.

Also, you can export the information on the Device Image Action Details page as a comma-separated values (CSV) file.

To export data on the Device Image Action Details page as a CSV file:

a. Click **Export as CSV**.

   You are prompted to save the file.

b. Click **OK** on the File Save page to save the file to your local file system.

c. After you save the file, to return to the Job Management page, click **OK** on the **Exporting Device Image Job** page.

Use an application such as Microsoft Excel to open the downloaded file from your local system. If you are using Microsoft Excel, you can filter data in the Status column to identify the devices on which the staging of images failed.

You can verify the checksum of the staged device image to ensure that the image is transferred completely to the device. For more information about how to verify the checksum, see "Verifying the Checksum" on page 630.

Release History Table

Release	Description
17.2	From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.

RELATED DOCUMENTATION

- Device Images Overview | **613**
- Staging Satellite Software Packages on Aggregation Devices | **625**
- Deploying Device Images | **637**
- Verifying the Checksum | **630**

Staging Satellite Software Packages on Aggregation Devices

Junos Space Network Management Platform enables you to stage satellite software packages to one or more Juniper Networks devices functioning as aggregation devices. Staging a package enables you to hold the package on a device, ready to be deployed when needed. At any given time, you can stage only a single satellite software package to an aggregation device. After you stage a satellite software package, you can verify the checksum to ensure that the package is transferred completely. For more information about aggregation devices and satellite devices, refer to the *Junos Fusion* documentation.

Satellite software packages have names prefixed with **satellite-** and must be downloaded and imported to Junos Space Platform before you can stage them. You can download satellite software packages from https://www.juniper.net/support/downloads/?p=fusion#sw.

To stage a satellite software package:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Images**.

   The Images page appears, displaying the software images imported to Junos Space Platform.

2. Select the satellite software package that you want to stage by selecting the check box beside the package name and select **Stage Image on Satellite Device** from the Actions menu.

   NOTE: The Stage Image on Satellite Device option is available on the Actions menu only if you select a satellite software package for staging.

The Stage Image on Satellite Devices page appears. The aggregation devices that are compatible with the selected package are listed.

This page displays the following information:

- **Image name**—Filename of the satellite software package that you have selected for staging
- **MD5 Value**—32-character hexadecimal number that is computed on the selected package, which is stored on the Junos Space server
- **Device Name**—Name of the discovered aggregation device, which is an identifier used for network communication between Junos Space Network Management Platform and the Junos OS device.
- **Domain**—Domain to which the aggregation device is assigned
- **IP Address**—IP address of the discovered aggregation device. For example, 10.1.1.1.
- **Platform**—Platform of the discovered aggregation device. For example, MX480.
- **Software Version**—Operating system firmware version running on the aggregation device. For example, 13.1X49D29.1.
- **Staged Status**—Indicates whether the selected package is staged on the discovered aggregation device. This column displays either **Staged** (if the package is staged) or **Not Staged** (if the package is not yet staged).
- **Checksum Status**—Indicates whether the satellite software package on the Junos Space server and the aggregation device is the same. The status can be one of the following:
  - **Valid** when the checksum values of the package on the Junos Space server and the aggregation device match
  - **Invalid** when the checksum values do not match
  - **NA** when the selected package is not staged on the aggregation device yet

  You can restage a package whose checksum status is “Invalid” to ensure that you stage the package onto the aggregation devices correctly, thereby making the checksum status “Valid.” You can deploy a package only when the checksum status is “Valid.”
- **Last Checksum Time**—Time when the checksum was last verified. For an aggregation device to which the selected package is not staged yet, this column displays **NA**.

> **NOTE:** You can verify the checksum for a satellite software package by selecting the **Verify Image on Devices** option from the Actions menu. For more information about how to verify the checksum, see “Verifying the Checksum” on page 630.

You can sort the data displayed in the following columns of the Stage Image on Satellite Devices page: **Device Name**, **IP Address**, **Platform**, **Software Version**, **Staged Status**, **Checksum Status**, and **Last Checksum Time**.

You can also filter the list of devices on the basis of the data in the following columns: **Device Name**, **IP Address**, **Platform**, and **Software Version**.

3. Select the aggregation device or devices to stage the satellite software package by using one of the following selection modes—manually, on the basis of tags, or by using a comma-separated values (CSV) file. These options are mutually exclusive. If you select one, the others are disabled.

   NOTE: By default, the **Select Device Manually** option is selected and the list of aggregation devices is displayed.

   To select devices manually:

   a. Click the **Select Device Manually** option, if it is not selected previously.

   b. Select the aggregation devices on which you want to stage the satellite software package.

      The Select Devices status bar shows the total number of aggregation devices that you selected. The status bar is dynamically updated as you select the devices.

   c. (Optional) To select all devices, select the check box in the column header next to Device Name.

   To select devices on the basis of tags:

   a. Click the **Select by Tags** option.

      The Select by tags list is activated.

   b. Click the arrow on the **Select by Tags** list.

      A list of tags defined for devices in Junos Space Platform appears, categorized into two—Public and Private.

      NOTE: If no tags are displayed, then it means that none of the aggregation devices is associated with any tag. You must first tag the aggregation devices on the Device Management page before you can use the **Select by Tags** option.

   c. To select tags, perform one of the following actions :

      - Select the check boxes next to the tag names to select the desired tags and click **OK**.

- To search for a specific tag, enter the first few letters of the tag name in the **Select by Tags** field to the left of the **OK** button. If a match is found, a suggestion is made. Select the suggested match and click **OK**.

As you select the tags, the total number of aggregation devices associated with the selected tags appears just above the device display table. For example, if there are six aggregation devices associated with the selected tags, then **6 items selected** is displayed.

The selected tags appear next to the **Tags Selected** label. An [X] icon appears after each tag name. You can click the [X] icon to clear any tag from the list. The device count decrements accordingly.

To select devices by using a CSV file:

a. Select the **Select by CSV** option.

b. Click **Browse** and select the file in the CSV format containing the list of aggregation devices to which you want to stage the package.

> **TIP:** For a sample CSV file, click the **Sample CSV** link. You are prompted to save the file. Save the file to your local system and open it by using an application, such as Microsoft Excel.

c. Click **Upload** to upload the CSV file.

From Release 16.1R2 onward, when you upload a CSV file to select devices from, Junos Space Platform verifies the devices in the CSV file. If the CSV file contains devices to which the changes do not apply, a warning message appears which says "Few devices are not selected due to precondition failure. Please click "View inapplicable devices" for more details." You can click the **View inapplicable devices** link to review the list of devices that are excluded from the update.

4. (Optional) To remove existing device images or satellite software packages from the device, expand the **Staging Options** section and select the **Delete any existing image before download** check box.

   When you delete a previously staged image, an audit log entry is automatically generated.

5. (Optional) To schedule a time for staging the satellite software package, select the **Schedule at a later time** check box and use the calendar icon and drop-down list to specify the date and time respectively.

6. Click **Stage Image**.

   The package is staged on the selected aggregation device or devices and a confirmation message appears, displaying the job ID. However, if the device on which you are trying to stage the satellite

software package does not have sufficient disk space to accommodate the package, then Junos Space displays an error message and the staging job fails.

> **NOTE:** The time taken to stage a package depends on the size of the package, network connectivity, and the number of devices on which the package is staged. You can monitor the progress of the staging job by viewing the **Percent** column of the particular job on the Job Management page.
>
> If Junos Space Platform detects an SSH fingerprint mismatch between that on the device and that in the Junos Space Platform database, the connection is dropped and the job fails. Connection Status displays Down and Authentication Status displays Fingerprint Conflict on the Device Management page.

To verify whether the package is staged successfully, click the ***job ID*** link or navigate to the Job Management page and view the status of the job. If staging fails on any of the devices, the job is a failure. You can double-click the job to view the reason for failure and the devices on which the job failed. The Device Image Action Details page appears, which displays the reason for failure in the **Description** column. However, if the package is staged successfully, then this column displays a success message.

You can export the information on the Device Image Action Details page as a comma-separated values (CSV) file.

To export data on the Device Image Action Details page as a CSV file:

a. Click **Export as CSV**.

   You are prompted to save the file.

b. Click **OK** in the File Save dialog box to save the file to your computer.

c. After you save the file, to return to the Job Management page, click **OK** in the **Exporting Device Image Job** dialog box.

Use an application such as Microsoft Excel to open the downloaded file from your computer. If you are using Microsoft Excel, you can filter data in the Status column to identify the devices on which the staging of packages failed.

You can verify the checksum of the staged satellite software package to ensure that the package is transferred completely to the device. For more information about how to verify the checksum, see "Verifying the Checksum" on page 630.

RELATED DOCUMENTATION

Device Images Overview | 613

Importing Device Images to Junos Space | 615

Deploying Satellite Software Packages on Aggregation and Satellite Devices | 652

Staging Device Images | 620

Verifying the Checksum

When you stage an image on a device by using Junos Space Network Management Platform, sometimes the device image is not completely transferred to the device. Verifying the checksum helps validate that the device image is staged properly and is not corrupted or altered in any way from the device image that you staged from the Junos Space server.

The checksum value is a 32-character hexadecimal number that is computed for the device image file on the device. The device image file is validated by verifying whether the checksum values stored on the Junos Space server and the device match. If the checksum values match, the device image is considered to be copied correctly.

> **NOTE:** You can verify the checksum of satellite software packages and Junos Continuity software packages by following the procedure for verifying the checksum of device images.

To verify the checksum:

1. On the Junos Space Network Management Platform UI, select **Images and Scripts** > **Images**.

   The Images page appears.

2. Select the image whose checksum you want to verify.

3. Select **Verify Image on Devices** from the Actions menu.

   This option is unavailable if you select multiple images for verifying the checksum. Select only one image and repeat this step.

   The Verifying checksum of image on device(s) page appears. This page displays the following information:

   - **Image name**—Name of the image, which you have selected for verifying the checksum
   - **MD5 Value**—32-character hexadecimal number that is computed on the selected device image file, which is stored on the Junos Space server

- **Host Name**—Name of the discovered device, which is an identifier used for network communication between Junos Space Network Management Platform and the Junos OS device
- **Device Alias**—Value of the Device Alias custom label for the device. This field is empty if the Device Alias custom label is not added or no value is assigned to the Device Alias custom label for the device.
- **IP Address**—IP address of the discovered device
- **Platform**—Platform of the discovered device
- **Serial Number**—Serial number of the device
- **Software Version**—Operating system firmware version running on the device
- **Staged Status**—Indicates whether the selected image is staged on the discovered device. This column displays either **Staged** (if the image is staged) or **Not Staged** (if the image is not yet staged).
- **Deployed Status**—Indicates whether the selected Junos Continuity software package is deployed on the device. This column appears only when you select a Junos Continuity software package for verifying the checksum. The column displays either **Deployed** (if the Junos Continuity software package is deployed) or **Undeployed** (if the Junos Continuity software package is not deployed).
- **Checksum Status**—Indicates whether the device image on the Junos Space server and the device are the same. The status can be one of the following:
  - **Valid** when the checksum values of the device image on the Junos Space server and the device match
  - **Invalid** when the checksum values of the device image on the Junos Space server and the device do not match
  - **NA** when the selected image is not staged on the device yet
- **Last Checksum Time**—Time when the checksum was last verified. For a device in which the selected image is not staged yet, this column displays **NA**. This column is updated when an image is restaged to the device.

4. Select the devices that have the device image staged on them by using one of the following selection modes—manually, on the basis of tags, or by using a comma-separated values (CSV) file. These options are mutually exclusive. If you select one, the others are disabled.

   TIP: Perform a validation on those devices where the **Checksum Status** column shows **Valid** but the **Last Checksum Time** column displays a time that is way past the current time. By performing this action, you ensure that the image on the devices is valid currently.

   NOTE: By default, the **Select by Device** option is selected and the complete list of devices is displayed.

To select devices manually:

a. Click the **Select Device Manually** option, if it is not selected previously.

b. Select the devices on which you want to verify the checksum.

   The Select Devices status bar shows the total number of devices that you selected. The status bar is dynamically updated as you select the devices.

c. To select all devices, select the check box in the column header next to Host Name.

To select devices on the basis of tags:

a. Click the **Select by Tags** option.

   The Select by tags list is activated.

b. Click the arrow on the **Select by Tags** list.

   A list of tags defined on devices in the Junos Space system appears, displaying two categories of tags—Public and Private.

   > **NOTE:** If no tags are displayed, then it means that none of the devices is associated with any tag. You need to tag the devices on the Device Management page before you can use the **Select by Tags** option.

c. To select tags, perform one of the following actions :

   - Select the check boxes next to the tag names to select the desired tags and click **OK**.
   - To search for a specific tag, enter the first few letters of the tag name in the **Select by Tags** field to the left of the **OK** button. If a match is found, a suggestion is made. Select the suggested match and click **OK**.

   As you select the tags, the total number of devices associated with the selected tags appears just above the device display table. For example, if there are six devices associated with the selected tags, then **6 items selected** is displayed.

   The selected tags appear next to the **Tags Selected** label. An [X] icon appears after each tag name. You can click the [X] icon to clear any tag from the list. The device count decrements accordingly.

   The device display table displays the devices associated with the selected tags.

From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.

To select devices by using a CSV file:

a. Select the **Select by CSV** option.

b. Click **Browse** to navigate to the file location in your local system and select the CSV file containing the list of devices on which you want to verify the device image.

> **TIP:** For a sample CSV file, click the **Sample CSV** link. You are prompted to save the file. Save the file to your local system and open it by using an application, such as Microsoft Excel.

c. Click **Upload** to upload the CSV file.

From Release 16.1R2 onward, when you upload a CSV file to select devices from, Junos Space Platform verifies the devices in the CSV file. If the CSV file contains devices to which the changes do not apply, a warning message appears which says **Few devices are not selected due to precondition failure. Please click "View inapplicable devices" for more details.**

You can click the **View inapplicable devices** link to review the list of devices that are excluded from the update. The reason for exclusion is listed as an error message against each device.

5. (Optional) To schedule a time for verifying the checksum, select the **Schedule at a later time** check box and use the calendar icon and drop-down list to specify the date and time respectively.

6. Click **Verify**.

The checksum value of the device image file on the Junos Space server is validated against the checksum value of the device image file stored on the selected devices. An alert appears, displaying the job ID.

To verify the devices on which the checksum status is valid, click the ***job ID*** link or navigate to the Job Management page and view the status of the job. If the job is a success, then the checksum values match on all devices selected for verification. However, if the job is a failure, double-click the row corresponding to the job to identify the devices on which this job is a failure. The Device Image Action Details displays the reason for failure in the **Description** column. Validation may fail if the checksum values do not match and for other reasons such as when the image is not staged on the device.

Also, you can export information from the Device Image Action Details page as a CSV file to your local system.

To export data from the Device Image Action Details page to your local system:

a. Click **Export as CSV**.

You are prompted to save the file.

b. Click **OK** in the File Save page to save the file to your local file system.

c. Click **OK** in the **Exporting Device Image Job** page, to return to the Job Management page.

Use an application such as Microsoft Excel to open the downloaded file from your local system. If you are using Microsoft Excel, you can filter data in the Status column to identify the devices on which the image verification failed.

When you verify a checksum, an audit log entry is automatically generated.

Release History Table

Release	Description
17.2	From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.

RELATED DOCUMENTATION

Device Images Overview | **613**

Viewing and Deleting MD5 Validation Results | **634**

Deploying Device Images | **637**

Viewing and Deleting MD5 Validation Results

IN THIS SECTION

- Viewing the MD5 Validation Results | **635**
- Deleting the MD5 Validation Results | **636**

Using Junos Space Network Management Platform, you can validate the completeness of a device image that is staged on the devices. If the checksum values of a device image file on the Junos Space server and the device match, then there is a high probability that the images are the same. The result of this validation appears on the Validation Results page. From this page, you can view and delete the validation results.

For more information about verifying the checksum, see “Verifying the Checksum” on page 630.

Viewing the MD5 Validation Results

The MD5 validation results indicate whether the device image that is staged on a device is completely transferred to the device or not. The result also indicates whether the device image is not present on the selected devices.

> **NOTE:** You can view the MD5 validation results of satellite software packages and Junos Continuity software packages by following the procedure for viewing the MD5 validation results of device images.

To view the MD5 validation results:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Images**.

   The Images page displays the list of device images.

2. Select a device image.

3. Select **MD5 Validation Result** from the Actions menu.

   The MD5 Validation Result page displays the results of verification tasks.

Table 70 describes the Validation Results page.

Table 70: Validation Results Page Field Descriptions

Field Name	Description
Device image name	Name of the device image selected for verifying the checksum
Device name	Name of the devices on which the device image is verified
Device Alias	Value of the Device Alias custom label for the device. This field is empty if the Device Alias custom label is not added or no value is assigned to the Device Alias custom label for the device.
Action	Name of the action performed
Checksum Result	Result of the verification
Remarks	Observations made during the verification. For example, “Validation Failed.”

Table 70: Validation Results Page Field Descriptions *(continued)*

Field Name	Description
Verification Time	Time at which you initiated verification by selecting **Verify Image on Devices** from the Actions menu

You can export the data from the Validation Results page as a CSV file to your local file system.

To export the data from the Validation Results page as a CSV file to your local file system:

1. Click **Export to CSV** from the Actions menu.

   You are prompted to save the file.

2. Click **OK** in the File Save dialog box to save the file to your local file system.

3. After you save the file, to return to the MD5 Validation Result page, click the [X] icon in the **Exporting Validation Results** dialog box to close the dialog box.

Navigate to the location where you saved the file and open the file by using an application such as Microsoft Excel. You can filter the data in the file to view the information you are interested in.

Deleting the MD5 Validation Results

> **NOTE:** You can delete the MD5 validation results of satellite software packages and Junos Continuity software packages by following the procedure for deleting the MD5 validation results of device images.

To delete the MD5 validation results:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Images**.

   The Images page appears.

2. Select a device image.

3. Select **MD5 Validation Result** from the Actions menu.

   The MD5 Validation Result page displays the results of all verification tasks.

4. Select the results that you want to delete.

5. Select **Delete Validation Results** from the Actions menu.

   The **Delete Validation Results** dialog box displays the selected results.

6. Click **Delete** to confirm.

   The selected results are removed from Junos Space Platform.

RELATED DOCUMENTATION

Device Images Overview | 613

Staging Device Images | 620

Verifying the Checksum | 630

Deploying Device Images

Junos Space Network Management Platform enables you to deploy device images and Junos Continuity software packages (JAM packages) onto a device or multiple devices of the same device family simultaneously. During deployment, a device image is installed on the device. Using an image that is already staged on a device eliminates the time taken to load the device image on a device and directly jumps to the installation process. Junos Space Network Management Platform also enables you to schedule a time when you want the image to be deployed.

> **NOTE:** Junos Space Platform enables you to deploy Junos Continuity software packages (JAM packages) on the MX240, MX480, MX960, MX2010, and MX2020 platforms. The filenames for Junos Continuity software packages are prefixed with **jam-** and are referred to as JAM packages in Junos Space Platform.
>
> From Junos Space Platform Release 18.2R1 onward, you can deploy VM host images on devices.

On dual Routing Engine platforms, you can also perform a unified in-service software upgrade (ISSU) between two different Junos OS software releases with no disruption on the control plane and with minimal disruption of traffic. This provides the following benefits:

- Eliminates network downtime during software image upgrades
- Reduces operating costs, while delivering higher service levels
- Allows fast implementation of new features

During the unified ISSU, the backup Routing Engine is rebooted with the new software package and switched over to make it the new primary Routing Engine. The former primary Routing Engine can also be upgraded to the new software and rebooted.

Table 71 describes the devices and software releases that support unified ISSU.

Table 71: Routing Platforms and Software Releases Supporting ISSU

Routing Platform	Software Release
M120 router	Junos 9.2 or later
M320 router	Junos 9.0 or later
MX Series Ethernet Services router **NOTE:** Unified ISSU for MX Series does not support IEEE 802.1ag OAM, IEEE 802.3ah, and LACP protocols.	Junos 9.3 or later
SRX Series Gateways	Junos 12.1 or later
T320 router	Junos 9.0 or later
T640 routing node	Junos 9.0 or later
T1600 routing node	Junos 9.1 or later
TX Matrix platform	Junos 9.3 or later

NOTE: EX Series switches do not support unified ISSU.

Additionally, you must note the following in connection with performing a unified ISSU:

- You can upgrade to a software version that supports unified ISSU from a software version that does not support unified ISSU only by means of a conventional upgrade. During the conventional upgrade, all line modules are reloaded, all subscribers are dropped, and traffic forwarding is interrupted until the upgrade is completed.
- The armed (upgrade) release must be capable of being upgraded to from the currently running release.
- All applications that are configured on the router must support unified ISSU and stateful SRP switchover.

- If one or more applications that do not support unified ISSU are configured, and you proceed with a unified ISSU, the unified ISSU process fails. To deploy the image on the device, you must choose a conventional upgrade on the router.
- To perform unified ISSU on an MX Series device, you must manually configure the device to enable Nonstop Bridging, in addition to GRES and NSR that Junos Space enables on the dual Routing Engine device for unified ISSU.

  NOTE: We strongly recommend that you configure the primary-only IP on the dual Routing Engine device. Dual Routing Engine devices without the primary-only configuration are not yet fully supported on Junos Space Platform. If the primary-only IP is not configured, physical inventory does not get listed after upgrading the dual Routing Engine device.

For more details about protocols, features, and PICs supported by unified ISSU, see the Unified ISSU System Requirements sections in the *Junos OS High Availability Configuration Guide*.

You can deploy a device image only onto devices or platforms supported by that device image. When you select an image for deployment, only those devices that are supported by the selected device image are displayed in the list of devices.

NOTE: In Junos Space Platform, an SRX Series cluster is represented as two individual devices with cluster peer information. When you deploy a device image on an SRX Series cluster, the image is installed on both cluster nodes.

NOTE: If you want to select **Check compatibility with current configuration** from the Conventional Deploy Options for an image on a dual Routing Engine device, make sure that GRES and NSR are disabled on the device.

Devices in an SRX Chassis Cluster can be upgraded by deploying device images from Junos Space Platform with a minimal service disruption of approximately 30 seconds using the In-band Cluster Upgrade (ICU) feature with the no-sync option. The ICU feature allows both devices in an SRX Chassis Cluster to be upgraded from the supported Junos OS versions. ICU is supported on SRX100, SRX110, SRX210, SRX220, SRX240, SRX300, SRX320, SRX340, SRX345, SRX550, and SRX650 Services Gateways if they run on Junos OS Releases 11.2R2 and later.

NOTE: You cannot upgrade the devices in an SRX Chassis Cluster using the ICU feature if Junos Space Platform cannot connect to one of the devices in the SRX Chassis Cluster. To ensure that you upgrade both devices on the SRX Chassis Cluster successfully:

- Select the **Remove the package after successful installation** check box in the Common Deployment Options, **Reboot device after successful installation** check box in the Conventional Deployment Options, and the check box next to ISSU Deployment Options during device image deployment.

NOTE:

- You can deploy Junos Continuity software packages on devices by following the procedure for deploying device images. Deployment options that are not relevant to Junos Continuity software do not appear when you select a Junos Continuity software package for deployment.
- You must ensure that the Modular Port Concentrators (MPCs) supported by the Junos Continuity software package are offline before you deploy the Junos Continuity software package to the devices from Junos Space Platform.

To deploy device images:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Images**.

   The Images page appears.

2. Select the image that you want to deploy.

   The selected image is highlighted.

3. Select **Deploy Device Image** from the Actions menu.

   The Deploy Image on Devices dialog box appears. The Select Devices table in the Deploy Image on Devices dialog box displays the devices that are supported by the selected device image. For a description of the fields in this table, see Table 72.

   Table 72: Select Devices Table Fields

Field	Description
Image name	Name of the device image. (This field is above the devices table.)
MD5 Value	32-character hexadecimal number that is computed on the selected device image file, which is stored on the Junos Space server
Device Name	Identifier used for network communication between Junos Space Platform and the device running Junos OS.
Device Alias	Value of the Device Alias custom label for the device. This field is empty if the Device Alias custom label is not added or no value is assigned to the Device Alias custom label for the device.
IP Address	IP address of the device.
Platform	Model number of the device.
Software Version	Operating system firmware version running on the device.
Staged Status	Indicates whether the selected image is staged on the discovered device. This column displays either **Staged** (if the image is staged) or **Not Staged** (if the image is not yet staged).
Deployed Status	Indicates whether the Junos Continuity software package is deployed on the device. This field appears only if you have selected a Junos Continuity software package to be deployed. The column displays either **Deployed** (if the Junos Continuity software package is deployed) or **Undeployed** (if the Junos Continuity software package is not deployed).

Table 72: Select Devices Table Fields *(continued)*

Field	Description
Checksum Status	Indicates whether the device image on the Junos Space server and the device are the same: • **Valid** means that the checksum values of the device image on the Junos Space server and the device match. • **Invalid** means that the checksum values of the device image on the Junos Space server and the device do not match. • **NA** means that the selected image is not staged on the device yet.
Last Checksum Time	Time when the checksum was last verified. For a device in which the selected image is not staged yet, this column displays **NA**.
Domain	Domain to which the device belongs

4. Select the devices on which you want to deploy the device image by using one of the following selection modes—manually, based on tags, or by using a comma-separated values (CSV) file. These options are mutually exclusive. If you select one, the others are disabled.

TIP:

Some points to consider when you select devices for deploying an image:

- Using a device in which the selected device image is already staged eliminates the time taken to load the device image on a device. However, if you select a device in which the image is not previously staged, then the deployment action stages the image first and then installs the image on the device. Use the **Staged** and **Not Staged** statuses on the **Staged Status** column to identify the devices in which the images are staged and not staged, respectively.
- If the **Last Checksum Time** value is way past the current time, it is better to verify the checksum before deploying the image so as to ensure that the image is valid. The deployment fails if the checksum values of the device image file on the Junos Space server and the device do not match. For more information about verifying the checksum, see "Verifying the Checksum" on page 630.

> **NOTE:** By default the **Select Device Manually** option is selected and the complete list of devices is displayed.

To select devices manually:

a. Click the **Select Device Manually** option, if it is not selected previously.

b. Select the devices on which you want to deploy the device image.

   The Select Devices status bar shows the total number of devices that you selected. The status bar is dynamically updated as you select the devices.

c. To select all devices, select the check box in the column header next to Device Name.

To select devices on the basis of tags:

a. Click the **Select by Tags** option. The Select by tags list is activated.

b. Click the arrow on the **Select by Tags** list. A list of tags defined for devices in Junos Space Platform appears, categorized into two—Public and Private.

> **NOTE:** If no tags are displayed, then it means that none of the devices is associated with any tag. You must tag the devices on the Device Management page before you can use the **Select by Tags** option.

c. To select tags, perform one of the following actions :

   - Select the check boxes next to the tag names to select the desired tags and click **OK**.
   - To search for a specific tag, enter the first few letters of the tag name in the **Select by Tags** field to the left of the **OK** button. If a match is found, a suggestion is made. Select the suggested match and click **OK**.

   As you select the tags, the total number of devices associated with the selected tags appears just above the device display table. For example, if there are six devices associated with the selected tags, then **6 items selected** is displayed.

The selected tags appear next to the **Tags Selected** label. An [X] icon appears after each tag name. You can click the [X] icon to clear any tag from the list. The device count decrements accordingly.

From Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.

To select devices by using a CSV file:

a. Select the **Select by CSV** option.

b. Click **Browse** and upload the file in CSV format containing the list of devices on which you want to deploy the device image.

> **TIP:** For a sample CSV file, click the **Sample CSV** link. You are prompted to save the file. Save the file to your local system and open it by using an application, such as Microsoft Excel.

From Release 16.1R2 onward, when you upload a CSV file to select devices from, Junos Space Platform verifies the devices in the CSV file. If the CSV file contains devices to which the changes do not apply, a warning message appears which says "Few devices are not selected due to precondition failure. Please click "View inapplicable devices" for more details." You can click the **View inapplicable devices** link to review the list of devices that are excluded from the update. The reason for exclusion is listed as an error message against each device.

5. (Optional) Select the **Show ISSU/ICU capable devices only** check box to display only those devices in which you can perform unified ISSU and ICU.

> **NOTE:** If you are deploying a Junos Continuity software package to the devices, the **Show ISSU/ICU capable devices only** check box is not available for selection.

6. To specify different deployment options, select one or more of the check boxes in the **Common Deployment Options**, **Conventional Deployment Options**, **ISSU Deployment Options**, and **Advanced Options** sections.

   See Table 73, Table 74, Table 75, and Table 76 for a description of the deployment options.

NOTE: When you perform a conventional upgrade of the device image on dual Routing Engines, the image is first deployed on the backup Routing Engine followed by the primary Routing Engine. If deployment fails on the backup Routing Engine, the device image is not deployed on the primary Routing Engine.

7. (Optional) To specify common deployment options, expand the **Common Deployment Options** section and select one or more check boxes. See Table 73 for a description of the common deployment options.

NOTE: If you are deploying a Junos Continuity software package to the devices, only the **Use image already downloaded to device** option is displayed in the **Common Deployment Options** section for selection.

Table 73: Common Deployment Options Descriptions

Common Deployment Options	Description
Use image already downloaded to device	Use the device image that is staged on the device for deployment.
Archive data (Snapshot)	Collect and save device data and executable areas. **NOTE:** If you are deploying a VM host image, this option is renamed as **Snapshot**.
Remove the package after successful installation	Delete the device image from the device after successful installation of the device image. **NOTE:** If you are deploying a VM host image, this option is disabled.
Delete any existing image before download	Delete all device images with the same filename from the device before deploying the selected device image.

8. (Optional) To specify conventional deployment options, expand the **Conventional Deployment Options** section and select one or more check boxes. See Table 74 for a description of the conventional deployment options.

NOTE: If you are deploying a Junos Continuity software package to the devices, the **Conventional Deployment Options** section is not available for selection.

Table 74: Conventional Deployment Options Descriptions

Conventional Deployment Options	Description
Check compatibility with current configuration	Verifies device image compatibility with the current configuration of the device
Upgrade Dual-Root Partition	Ensures that the device image is deployed to both the primary and the backup root partitions of devices with dual-root partitions. This option is available for EX, ACX, and SRX Series (SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650 Services Gateway) devices only. By default, the device image is deployed only to the primary root partition. You must select the check box to deploy the device image to both the primary and the backup root partitions. The **Upgrade Dual-Root Partition** is available from Junos Space Network Management Platform Release 16.1R1 onward. **NOTE:** If you are deploying a VM host image, this option is disabled.
Load succeeds if at least one statement is valid	Ensures that the device image is loaded successfully even if only one of the selected deployment options is valid **NOTE:** If you are deploying a VM host image, this option is disabled.
Reboot device after successful installation	Reboots the device after deployment is successful. If the device is down, Junos Space Platform waits for the device to come up before initiating the reboot. If the device is not up within 30 minutes, the Image Deployment Job is marked as failed. After rebooting the device, the status of the device is checked every five minutes to check whether the device is up. **NOTE:** This check box is automatically selected when you select the Upgrade Dual-Root Partition option. You must not clear this check box if the Upgrade Dual-Root Partition option is selected.
Force Host Upgrade	Upgrades the host OS and Junos OS of the device. **NOTE:** This option is enabled only for ACX, QFX, and EX Series devices and the image being deployed must contain host OS packages. If you enable this option, the **ISSU Deployment Options** cannot be enabled. If you are deploying a VM host image, this option is disabled.

Table 74: Conventional Deployment Options Descriptions *(continued)*

Conventional Deployment Options	Description
Upgrade Backup Routing Engine only	Deploys the image to only the backup Routing Engine
Dual-Root Partitioning for SRX	Supports dual partition for SRX Series devices This check box is disabled for non-SRX Series devices. **NOTE:** If you are deploying a VM host image, this option is disabled.

9. (Optional) To perform unified ISSU on a dual Routing Engine device, expand the **ISSU Deployment Options** section and select one or more of the check boxes. The ISSU option is enabled only if the selected device has a dual Routing Engine. For devices with dual Routing Engines the term **Dual RE** is displayed in the **Platform** column of the **Select Devices** table on the Deploy Images on Devices page.

   NOTE: If you are deploying a Junos Continuity software package to the devices, the **ISSU Deployment Options** section is not available for selection.

   See Table 75 for a description of the unified ISSU deployment options.

   Table 75: Unified ISSU Deployment Options Descriptions

Unified ISSU Deployment Options	Description
Upgrade the former Master with new image	After the backup Routing Engine is rebooted with the new software package and a switchover occurs to make it the new primary Routing Engine; the former primary (new backup) Routing Engine is automatically upgraded. If you do not select this option, the former primary Routing Engine must be manually upgraded.
Reboot the former Master after a successful installation	The former primary (new backup) Routing Engine is rebooted automatically after being upgraded to the new software. If this option is not selected, you must manually reboot the former primary (new backup) Routing Engine.
Save copies of the package files on the device	Copies of the package files are retained on the device. **NOTE:** If you are deploying a VM host image, this option is disabled.

10. (Optional) To specify advanced deployment options, expand the **Advanced Options** and select one or more check boxes. See Table 76 for a description of the advanced deployment options. From this section, you can execute script bundles before and after image deployment.

> **NOTE:** If you are assigned a user role that does not have the permissions required for executing script bundles on devices, then all the options in the **Advanced Options** section are unavailable.

Table 76: Advanced Options Descriptions

Advanced Options	Description
Execute script bundle before image deployment (pre scripts)	Execute the script bundle that you have selected before deploying the device image. This ensures that the scripts in the selected script bundle are executed before the device image is installed on the device. After selecting a script bundle, you can configure the script parameters of the scripts within the script bundle (for instructions, see the following procedure starting with Step a).
Select same pre script bundle for post script bundle	Execute the same script bundle on the device before and after device image deployment. This check box is unavailable if you have not selected a script bundle on the **Execute script bundle before image deployment (pre scripts)** list.
Execute script bundle after image deployment (post scripts)	Execute the selected script bundle after deploying the device image. This ensures that the scripts in the selected script bundle are executed after the device image is installed on the device. After selecting a script bundle, you can configure the script parameters of the scripts within the script bundle (for instructions, see the following procedure starting with Step a). If you selected the **Select same pre script bundle for post script bundle** check box, then the **Execute script bundle after image deployment (postscripts)** check box is unavailable because the postscript bundle is the same as the prescript bundle.

Table 76: Advanced Options Descriptions *(continued)*

Advanced Options	Description
Deploy and Enable script bundle before execution	Deploy the selected script bundle, enable the scripts included in the script bundle, and then execute the script bundle on the device. If you are assigned a user role that does not have permissions for staging or enabling script bundles on devices, this check box is unavailable for selection. This check box is also unavailable if you have not selected a script bundle on the **Execute script bundle before image deployment (pre scripts)** list or the **Execute script bundle after image deployment (post scripts)** list.
Disable scripts after execution	Execute the scripts in the script bundle on the device and then disable the scripts in the script bundle. You can enable the scripts at a later point of time (for instructions, see "Enabling Scripts on Devices" on page 696). If you are assigned a user role that does not have permissions for disabling script bundles on devices, this check box is unavailable for selection.

To configure the script parameters of scripts included in the script bundle:

a. Select the prescript or postscript bundle that you want to configure, from the respective lists.

   If there are no script bundles listed, you can create script bundles using the Scripts workspace (see "Creating a Script Bundle" on page 750) and then select the script bundle during image deployment.

b. Click the **Configure Scripts Parameters** link.

   The Configure Script Bundle Parameters page appears. You can hover over the script parameters to view short descriptions about them.

c. You can edit the value of script parameters by clicking the icon before deploying the script bundle on the devices. The changes made to script parameters are saved only on the devices on which the script bundle is executed. The script parameters in the script bundle in Junos Space Platform continue to reflect the original values.

d. Click **Configure**.

Your changes are saved and the Deploy Image on Devices page appears.

11. (Optional) To schedule a time for deployment, select the **Schedule at a later time** check box and use the calendar icon and drop-down list to specify the date and time respectively.

12. Click **Deploy**.

    The selected image is deployed on the specified devices with the deployment options that you specified and an alert appears, displaying the job ID.

    NOTE: You can monitor the progress of completion from the **Percent** column of the particular job on the Job Management page. If Junos Space Platform detects an SSH fingerprint mismatch between that on the device and that in the Junos Space Platform database, the connection is dropped. The Connection Status displays Down and Authentication Status displays Fingerprint Conflict on the Device Management page. The View Job Details page displays an error message.

    NOTE: After you deploy Junos Continuity software packages from Junos Space Platform to devices, you must ensure that the Modular Port Concentrators (MPCs) supported by the Junos Continuity software package are in the online state.

    To verify whether the image is deployed successfully, click the ***job ID*** link or navigate to the Job Management page and view the status of the job. If the job is a failure, you can double-click the row corresponding to the job to view the reason for failure. If there is an error, the View Job Details page displays an error message. For more information about the error messages, see "Common Error Messages in Device-Related Operations" on page 992.

    The Device Image Action Details page displays the reason for failure in the **Description** column. However, if the image is deployed successfully, then this column displays information that is similar to the following text depending on the image and the device to which the image is deployed:
    Image [12.3R1.7] to be deployed :jinstall-12.3R1.7-domestic-signed.tgz.
    Gathered Routing Engine Information.
    Package installed on backup RE.
    Backup RE rebooted.
    Gathered software version information from backup RE.
    Package installed on master RE.
    Master RE rebooted.
    Gathered software version information.

NOTE: If you choose to deploy the device image only on the primary root partition of a device with dual-root partitions, the detailed job summary of the corresponding job displays a warning that you must use the **request system snapshot slice alternate** command on the device to copy the device image to the alternative root partition.

Also, you can export information from the Device Image Action Details page as a comma-separated values (CSV) file to your local file system.

To export data from the Device Image Action Details page to your local file system:

a. Click **Export as CSV**.

   You are prompted to save the file.

b. Click **OK** on the File Save dialog box to save the file to your local file system.

c. After you save the file, to return to the Job Management page, click **OK** on the **Exporting Device Image Job** dialog box.

Use an application such as Microsoft Excel to open the downloaded file from your local system. If you are using Microsoft Excel, you can filter data in the Status column to identify the devices on which the image deployment failed. See the associated Description column to understand the reasons for failure.

You can also view the result of deployment from the View Deploy Results page. See "Viewing Device Image Deployment Results" on page 657.

Release History Table

Release	Description
18.2	From Junos Space Platform Release 18.2R1 onward, you can deploy VM host images on devices.
17.2	From Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.
16.1R1	The **Upgrade Dual-Root Partition** is available from Junos Space Network Management Platform Release 16.1R1 onward.

RELATED DOCUMENTATION

Device Images Overview | 613
Importing Device Images to Junos Space | 615
Deploying Satellite Software Packages on Aggregation and Satellite Devices | 652
Script Bundles Overview | 749

Deploying Satellite Software Packages on Aggregation and Satellite Devices

Junos Space Network Management Platform enables you to deploy satellite software packages to one or more Juniper Networks devices functioning as aggregation devices and to the satellite devices connected to these aggregation devices simultaneously. When you deploy a satellite software package, the package is installed on the selected aggregation devices and connected satellite devices. If the satellite software package is already staged on the devices, the time taken to load the package is eliminated and Junos Space Platform directly installs the package. Junos Space Platform also enables you to schedule the deployment of a package at a later time.

You can deploy a satellite software package only onto devices or platforms supported by that package. When you select a satellite software package for deployment, only those devices that are supported by the selected package are displayed on the list of aggregation devices.

Satellite software packages have names prefixed with **satellite-** and must be downloaded and imported to Junos Space Platform before you can deploy them. You can download satellite software packages from https://www.juniper.net/support/downloads/?p=fusion#sw.

> **NOTE:** Junos Space deploys satellite package onto a satellite device through an aggregation device by upgrading all software upgrade groups on the aggregation device rather than the corresponding satellite software upgrade group.

To deploy satellite software packages:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Images**.

   The Images page appears, displaying the software images imported to Junos Space Platform.

2. Select the satellite software package that you want to deploy by selecting the check box beside the package name.

   The selected package is highlighted.

3. Select **Deploy Satellite Device Image** from the Actions menu.

NOTE: The Deploy Satellite Device Image option is available on the Actions menu only if you select a satellite software package for staging.

The Deploy Image on Satellite Devices dialog box appears. The Select Devices table in the Deploy Image on Satellite Devices dialog box displays the aggregation devices that are supported by the selected satellite software package. For a description of the fields in this table, see Table 77.

Table 77: Select Devices Table Fields

Field	Description
Image name	Filename of the satellite software package. (This field is above the devices table.)
MD5 Value	32-character hexadecimal number that is computed on the selected satellite software package, which is stored on the Junos Space server
Device Name	Identifier used for network communication between Junos Space Platform and the device running Junos OS
IP Address	IP address of the aggregation device
Platform	Model number of the aggregation device
Software Version	Operating system firmware version running on the aggregation device
Staged Status	Indicates whether the selected package is staged on the aggregation device. This column displays either **Staged** (if the package is staged) or **Not Staged** (if the package is not yet staged).
Checksum Status	Indicates whether the satellite software package on the Junos Space server and the aggregation device are the same: • **Valid** means that the checksum values of the package on the Junos Space server and the device match. • **Invalid** means that the checksum values of the package on the Junos Space server and the device do not match. • **NA** means that the selected package is not staged on the device yet.
Last Checksum Time	Time when the checksum was last verified. For a device in which the selected package is not staged yet, this column displays **NA**.
Domain	Domain to which the aggregation device belongs

4. Select the devices on which you want to deploy the satellite software package by using one of the following selection modes—manually, on the basis of tags, or by using a comma-separated values (CSV) file. These options are mutually exclusive. If you select one, the others are disabled.

   TIP:

   Some points to consider when you select devices for deploying a package:

   - Using a device on which the selected satellite software package is already staged eliminates the time taken to load the package on a device. However, if you select a device on which the package is not previously staged, then the deployment action stages the package first and then installs the package on the device. Use the **Staged** and **Not Staged** statuses in the **Staged Status** column to identify the devices on which the packages are staged and not staged, respectively.
   - If the **Last Checksum Time** value shows that the checksum is not verified recently, it is better to verify the checksum again before deploying the package so as to ensure that the package is valid. The deployment fails if the checksum values of the satellite software package file on the Junos Space server and the device do not match. For more information about verifying the checksum, see "Verifying the Checksum" on page 630.

   NOTE: By default, the **Select Device Manually** option is selected and the list of aggregation devices is displayed.

   To select devices manually:

   a. Click the **Select Device Manually** option, if it is not selected previously.

   b. Select the devices on which you want to deploy the satellite software package.

      The Select Devices status bar shows the total number of aggregation devices that you selected. The status bar is dynamically updated as you select the devices.

   c. To select all devices, select the check box in the column header next to Device Name.

   To select devices on the basis of tags:

   a. Click the **Select by Tags** option.

      The Select by tags list is activated.

   b. Click the arrow on the **Select by Tags** list.

A list of tags defined for devices in Junos Space Platform appears, categorized into two—Public and Private.

> **NOTE:** If no tags are displayed, then it means that none of the devices is associated with any tag. You must tag the devices on the Device Management page before you can use the **Select by Tags** option.

c. To select tags, perform one of the following actions :

- Select the check boxes next to the tag names to select the desired tags and click **OK**.
- To search for a specific tag, enter the first few letters of the tag name in the **Select by Tags** field to the left of the **OK** button. If a match is found, a suggestion is made. Select the suggested match and click **OK**.

As you select the tags, the total number of aggregation devices associated with the selected tags appears just above the device display table. For example, if there are six aggregation devices associated with the selected tags, then **6 items selected** is displayed.

The selected tags appear next to the **Tags Selected** label. An [X] icon appears after each tag name. You can click the [X] icon to clear any tag from the list. The device count decrements accordingly.

To select devices by using a CSV file:

a. Select the **Select by CSV** option.

b. Click **Browse** and select the file in the CSV format containing the list of aggregation devices on which you want to deploy the satellite software package.

> **TIP:** For a sample CSV file, click the **Sample CSV** link. You are prompted to save the file. Save the file to your local system and open it by using an application, such as Microsoft Excel.

c. Click **Upload** to upload the CSV file.

From Release 16.1R2 onward, when you upload a CSV file to select devices from, Junos Space Platform verifies the devices in the CSV file. If the CSV file contains devices to which the changes do not apply, a warning message appears which says "Few devices are not selected due to

precondition failure. Please click "View inapplicable devices" for more details." You can click the **View inapplicable devices** link to review the list of devices that are excluded from the update.

5. (Optional) To specify common deployment options, expand the **Common Deployment Options** section and select one or more check boxes. See Table 78 for a description of the common deployment options.

   Table 78: Common Deployment Options Descriptions

Common Deployment Options	Description
Use image already downloaded to device	Use the satellite software package that is staged on the devices for deployment.
Archive data (Snapshot)	Collect and save device data and executable areas to the snapshot locations for the device, such as **/altroot**, **/altconfig**, **/config**, and so on.
Remove the package after successful installation	Delete the satellite software package from the devices after the successful installation of the package.
Delete any existing image before download	Delete all satellite software packages with the same filename from the device before deploying the selected package.

6. (Optional) To schedule a time for deployment, select the **Schedule at a later time** check box and use the calendar icon and drop-down list to specify the date and time respectively.

7. Click **Deploy**.

   The selected package is deployed on the selected aggregation devices and the connected satellite devices, with the deployment options that you specified, and an alert appears, displaying the job ID.

   > **NOTE:** You can monitor the progress of completion from the **Percent** column of the particular job on the Job Management page. If Junos Space Platform detects an SSH fingerprint mismatch between that on the device and that in the Junos Space Platform database, the connection is dropped and the job fails. Connection Status displays Down and Authentication Status displays Fingerprint Conflict on the Device Management page.

   To verify whether the package is deployed successfully, click the ***job ID*** link or navigate to the Job Management page and view the status of the job. If the deployment fails on any of the devices, the job is a failure. You can double-click the job to view the reason for failure and the devices on which the job failed. The Device Image Action Details page displays the reason for failure in the **Description** column. However, if the package is deployed successfully, then this column displays a success message.

Also, you can export information from the Device Image Action Details page as a comma-separated values (CSV) file to your local file system.

To export data from the Device Image Action Details page to your local file system:

a. Click **Export as CSV**.

   You are prompted to save the file.

b. Click **OK** in the File Save dialog box to save the file to your local file system.

c. After you save the file, to return to the Job Management page, click **OK** in the **Exporting Device Image Job** dialog box.

Use an application such as Microsoft Excel to open the downloaded file from your local system. If you are using Microsoft Excel, you can filter data in the Status column to identify the devices on which the package deployment failed. See the associated Description column to understand the reasons for failure.

You can also view the result of deployment from the View Deploy Results page. For more information, see "Viewing Device Image Deployment Results" on page 657.

RELATED DOCUMENTATION

Device Images Overview | 613

Importing Device Images to Junos Space | 615

Staging Satellite Software Packages on Aggregation Devices | 625

Deploying Device Images | 637

Viewing Device Image Deployment Results

Junos Space Network Management Platform enables you to view the results of device image deployment. You can also filter the results to display only those instances where deployment failed.

NOTE: You can view the deployment results for satellite software packages and Junos Continuity software packages by following the procedure for viewing deployment results for device images.

To view deployment results:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Images**.

   The Images page appears.

2. Click the **View Deployed Results** icon.

   The View Deployed Results page appears, displaying the job ID, scheduled start time, name of the image, job description, script bundles executed, actual start time, end time, and the results of the deployment job. The columns on this page can be displayed or hidden as required.

   To display or hide a column:

   a. Click the down arrow on any column header.

   b. Select **Columns**.

      A list with menu options corresponding to all available column headings appears with a check box next to each heading. The check boxes for the headings that are displayed are selected; those that are hidden are not selected.

   c. Select or deselect the headings as desired.

      The tabular view changes to reflect your choices.

3. (Optional) To view only the failures in deployment, select the **Show Failures** check box. By default, this check box is unselected.

   If the check box is selected, then the View Deployed Results page displays only the deployment jobs that failed.

4. (Optional) To view more information about the status of a job:

   a. On the View Deployed Results page, select a job.

   b. In the **Results** column, click the **SUCCESS** or **FAILURE** link.

      The Image Deploy Results page appears, displaying the following information:

      - **Image Name**—Deployed image name
      - **Job Id**—Deployment job ID
      - **Result**—Indicates whether the deployment is a success or failure
      - **Summary**—Deployment options that you selected while deploying the image
      - **Hostname**—Device to which the image is deployed
      - **Comment**—More information about the status of the job

Example text, which is displayed when a deployment job is a failure:
Image [12.3R3.4] to be deployed: jinstall-ex-3300-12.3R3.4-domestic-signed.tgz
Gathered Routing Engine Information.
Failed to execute RPC request-package-add in 1024.134 seconds.
Error message from Device: null

Example text, which is displayed when a deployment job is a success:
Image [11.4R7.5] to be deployed: junos-srx1k3k-11.4R7.5-doemstic.tgz
Completed copying file to the device.
Package installed on device.
Device rebooted.
Gathered software version information.

c. (Optional) To determine whether the scripts that you chose to execute before and after image deployment were successfully executed, click the arrow next to the hostname.

   Two tables appear, which display a list of prescripts and postscripts and whether they were successfully executed.

d. Click **Close** on the Image Deploy Results page to return to the View Deployed Results page.

5. Click the **Images** breadcrumb at the top of the View Deployed Results page to return to the Images page.

RELATED DOCUMENTATION

Deploying Device Images | 637
Staging Device Images | 620

Viewing Device Association of Images

You can view the images that are staged to a single device or multiple devices running Junos OS by using Junos Space Network Management Platform. You can view the device associations for one or more images from the Images page. On the Images page, click **View** in the **Associations** column of an image entry to view the associated devices for that image.

> **NOTE:** You can view the device association of satellite software packages and Junos Continuity software packages by following the procedure for viewing the device association of device images.

To view devices on which an image is staged:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Images**.

   The Images page appears.

2. Select an image.

   > **NOTE:** Junos Space does not display images that are staged out-of-band.

3. Select **View Associated Devices** from the Actions menu or click **View** in the **Associations** column.

   The View Associated Devices page appears with valid image–device association details, which include the image name, the device name, device alias custom label, IP address, platform, software version, and staged status of the devices. If you are viewing the device associations of a Junos Continuity software package, the deployed status is also displayed. This page is read-only and hence you cannot perform any actions on this page.

   > **NOTE:** The image(–)device(s) association details are displayed only if you stage an image on to devices in Junos Space Release 13.3R1 or later versions. If you staged an image on to a device by using a version prior to Junos Space Release 13.3R1 and then upgraded to Release 13.3R1 or later versions, then this image(–)device(s) association is not displayed.

4. Click **Back** at the top of the View Associated Devices page.

You are now returned to the Images page.

RELATED DOCUMENTATION

- Deploying Device Images | **637**
- Staging Device Images | **620**
- Device Images Overview | **613**

Undeploying JAM Packages from Devices

Junos Space Network Management Platform allows you to undeploy Junos Continuity software packages (JAM packages) that you have earlier deployed to devices. When you undeploy the Junos Continuity software package using the **Undeploy JAM Package from Device** action, the package is uninstalled from the selected device or devices.

> **NOTE:** You must ensure that the Modular Port Concentrators (MPCs) supported by the Junos Continuity software package are offline before you undeploy the Junos Continuity software package from the devices by using Junos Space Platform.

To undeploy the Junos Continuity software package from devices:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Images**.

   The Images page appears.

2. Select the check box beside the entry for the Junos Continuity software package that you want to undeploy.

3. Select **Undeploy JAM Package from Device** from the Actions menu.

   The **Undeploy JAM Package from Device** dialog box appears. The Select Devices table in the Undeploy JAM Package from Device dialog box displays the devices that are supported by the selected Junos Continuity software package. For a description of the fields in this table, see Table 79

   Table 79: Select Devices Table Fields

Field	Description
JAM Package Name	Name of the Junos Continuity software package (This field is above the devices table.)
MD5 Value	32-character hexadecimal number that is computed on the selected Junos Continuity software package file, which is stored on the Junos Space server
Device Name	Identifier used for network communication between Junos Space Platform and the device running Junos OS
Device Alias	Value of the Device Alias custom label for the device. This field is empty if the Device Alias custom label is not added or no value is assigned to the Device Alias custom label for the device.
IP Address	IP address of the device

Table 79: Select Devices Table Fields *(continued)*

Field	Description
Platform	Model number of the device
Software Version	Operating system firmware version running on the device
Staged Status	Indicates whether the selected Junos Continuity software package is staged on the device. This column displays either **Staged** (if the Junos Continuity software package is staged) or **Not Staged** (if the Junos Continuity software package is not staged).
Deployed Status	Indicates whether the Junos Continuity software package is deployed on the device. The column displays either **Deployed** (if the Junos Continuity software package is deployed) or **Undeployed** (if the Junos Continuity software package is not deployed).
Checksum Status	Indicates whether the Junos Continuity software package on the Junos Space server and the device are the same: • **Valid** means that the checksum values of the Junos Continuity software package on the Junos Space server and the device match. • **Invalid** means that the checksum values of the Junos Continuity software package on the Junos Space server and the device do not match. • **NA** means that the selected Junos Continuity software package is not staged on the device yet.
Last Checksum Time	Time when the checksum was last verified. For a device in which the selected Junos Continuity software package is not staged yet, this column displays **NA**.
Domain	Domain to which the device belongs

4. Select the devices from which you want to undeploy the Junos Continuity software package by using one of the following selection modes—manually, based on tags, or by using a comma-separated values (CSV) file. These options are mutually exclusive. If you select one, the others are disabled.

   NOTE: By default, the **Select Device Manually** option is selected and the list of devices on which the Junos Continuity software package is deployed is displayed.

   To select devices manually:

   a. Click the **Select Device Manually** option button, if it is not selected previously.

   b. Select the devices from which you want to undeploy the Junos Continuity software package.

The Select Devices status bar shows the total number of devices that you selected. The status bar is dynamically updated as you select devices.

c. To select all devices, select the check box in the column header next to Device Name.

To select devices on the basis of tags:

a. Click the **Select by Tags** option button.

The Select by tags list is activated.

b. Click the arrow on the **Select by Tags** list.

A list of tags defined for devices in the Junos Space system appears, categorized into two—Public and Private.

> **NOTE:** If no tags are displayed, then it means that none of the devices is associated with any tag. You must first tag the devices on the Device Management page before you can use the **Select by Tags** option.

c. To select tags, perform one of the following actions :

- Select the check boxes next to the tag names to select the desired tags and click **OK**.
- To search for a specific tag, enter the first few letters of the tag name in the **Select by Tags** field to the left of the **OK** button.If a match is found, a suggestion is made. Select the suggested match and click **OK**.

As you select the tags, the total number of devices associated with the selected tags, on which the selected Junos Continuity software package is deployed, appears just above the device display table. For example, if there are six devices associated with the selected tags, and two of them have the selected Junos Continuity software package deployed, then **2 items selected** is displayed.

The selected tags appear next to the **Tags Selected** label. An [X] icon appears after each tag name. You can click the [X] icon to clear any tag from the list. The device count decrements accordingly.

To select devices by using a CSV file:

a. Select the **Select by CSV** option button.

b. Click **Browse** and upload the file in CSV format containing the list of devices from which you want to undeploy the Junos Continuity software package.

> **TIP:** For a sample CSV file, click the **Sample CSV** link. You are prompted to save the file. Save the file to your local system and open it by using an application, such as Microsoft Excel.
>
> From Release 16.1R2 onward, when you upload a CSV file to select devices from, Junos Space Platform verifies the devices in the CSV file. If the CSV file contains devices to which the changes do not apply, a warning message appears which says "Few devices are not selected due to precondition failure. Please click "View inapplicable devices" for more details." You can click the **View inapplicable devices** link to review the list of devices that are excluded from the update.

5. (Optional) To specify advanced options, expand the **Advanced Options** and select one or more check boxes.

   Using the options in this section, you can specify the script bundles to be executed before and after undeploying the Junos Continuity software package. See Table 80 for a description of the advanced options.

   > **NOTE:** If you are assigned a user role that does not have the permissions required for executing script bundles on devices, then all the options in the **Advanced Options** section are unavailable.

   Table 80: Advanced Options Description

Advanced Options	Description
Execute script bundle before JAM Package undeployment (pre scripts)	Execute the script bundle that you have selected from the list, before undeploying the Junos Continuity software package. This ensures that the scripts in the selected script bundle are executed before the Junos Continuity software package is uninstalled from the device. After selecting a script bundle, you can configure the script parameters of the scripts within the script bundle. For instructions, see the following procedure starting with Step a.
Select same pre script bundle for post script bundle	Execute the same script bundle on the device before and after the Junos Continuity software package is undeployed. This check box is unavailable if you have not selected a script bundle on the **Execute script bundle before JAM Package undeployment (pre scripts)** list.

Table 80: Advanced Options Description *(continued)*

Advanced Options	Description
Execute script bundle after JAM Package undeployment (post scripts)	Execute the script bundle that you have selected from the list, after undeploying the Junos Continuity software package. This ensures that the scripts in the selected script bundle are executed after the Junos Continuity software package is uninstalled from the device. After selecting a script bundle, you can configure the script parameters of the scripts within the script bundle. For instructions, see the following procedure starting with Stepa. If you select the **Select same pre script bundle for post script bundle** check box, then the **Execute script bundle after JAM Package undeployment (post scripts)** check box is unavailable because the postscript bundle is the same as the prescript bundle.
Deploy and Enable script bundle before execution	Deploy the selected script bundle and enable the scripts included in the script bundle before the script bundle is executed on the device. If you are assigned a user role that does not have permissions for staging or enabling script bundles on devices, this check box is unavailable for selection. This check box is also unavailable if you have not selected a script bundle on the **Execute script bundle before JAM Package undeployment (pre scripts)** list or the **Execute script bundle after JAM Package undeployment (post scripts)** list.
Disable scripts after execution	Disable the scripts in the script bundle after they are executed on the device. If you are assigned a user role that does not have permissions for disabling script bundles on devices, this check box is unavailable for selection. You can enable the scripts at a later point of time (for instructions see "Enabling Scripts on Devices" on page 696).

To configure the script parameters of scripts included in the script bundle:

a. Select the prescript or postscript bundle that you want to configure, from the respective lists.

   If there are no script bundles listed, you can create script bundles using the Scripts workspace (see "Creating a Script Bundle" on page 750) and then select the script bundle during Junos Continuity software package undeployment.

b. Click the **Configure Scripts Parameters** link.

   The Configure Script Bundle Parameters page appears. You can mouse over the script parameters to view short descriptions about them.

c. Edit the values of script parameters by clicking the Edit icon.

   The changes made to script parameters are saved only on the devices on which the script bundle is executed. The script parameters in the script bundle in Junos Space Platform continue to reflect the original values.

d. Click **Configure**.

   Your changes are saved and the Undeploy JAM Package from Device dialog box appears.

6. (Optional) To schedule a time for deployment, select the **Schedule at a later time** check box and use the calendar icon and drop-down list to specify the date and time respectively.

7. Click **Undeploy**.

   The Job Information dialog box appears with a message indicating that the undeploy job is successfully scheduled. You can click the ***job ID*** link that is displayed in the dialog box if you want to view the job details. You can also navigate to the Job Management page and view the details of the particular job.

8. Click **OK**.

   You are returned to the **Images** page.

When you undeploy a JAM package from a device, an audit log entry is automatically generated. You can view the audit logs from the Audit Logs workspace.

RELATED DOCUMENTATION

- Device Images Overview | **613**
- Importing Device Images to Junos Space | **615**
- Staging Device Images | **620**
- Deploying Device Images | **637**

Removing Device Images from Devices

Before you can delete device images from Junos Space Network Management Platform, you must remove the device images from the devices on which they are staged or deployed. Junos Space Platform does not allow you to remove images that are associated with a device.

NOTE: You can remove satellite software packages and Junos Continuity software packages from devices by following the procedure for removing device images.

To remove device images from the devices on which they are staged:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Images**.

   The Images page appears, displaying the device images in Junos Space Platform.

2. Select the images that you want to remove.

   The selected images are highlighted.

3. Select **Remove Staged Image from Device** from the Actions menu.

   If the selected images are not staged on any of the devices, then Junos Space Platform displays the following error message:
   None of the device(s) have all the selected image(s) staged.

   If there is at least one device on which the images are staged, then the Remove Image from Staged Devices page appears. Only the devices on which all the selected images are staged are displayed. For example, Image1 is staged on DeviceA and DeviceB, and Image2 is staged on DeviceA. When you select Image1 and Image2 for deletion, the Remove Image from Staged Devices page displays only DeviceA. This is because only DeviceA is common to both Image1 and Image2.

   TIP: Before you proceed to delete an image from the devices, ensure that the **Device Image name(s)** field displays the name of the image that you want to delete. If the name of a different image is displayed, click the **Images** breadcrumb at the top of the page to return to the Images page and select the correct image.

Table 81 gives the descriptions of fields displayed in the Remove Image from Staged Devices page.

Table 81: Remove Image from Staged Devices page Fields

Fields	Description
Device Image name(s)	Name of the image that you want to delete from the devices. If you select multiple images to delete, then the names of all selected images are displayed.
Device Name	Name of the device from which you can delete the image

Table 81: Remove Image from Staged Devices page Fields *(continued)*

Fields	Description
Device Alias	Value of the Device Alias custom label for the device. This field is empty if the Device Alias custom label is not added or no value is assigned to the Device Alias custom label for the device.
IP Address	IP address of the device
Platform	Platform of the device, such as MX480, MX320, MX960, and so on
Software Version	Version of software running on the device, such as 12.3R2.5, 11.2R3.3, and so on

4. Select the devices from which you want to delete the image by using one of the following selection modes—manually, based on tags, or by using a comma-separated values (CSV) file. These options are mutually exclusive. If you select one, the others are disabled.

   NOTE: By default, the **Select Device Manually** option is selected and the list of devices on which the image is staged is displayed.

   To select devices manually:

   a. Click the **Select Device Manually** option, if it is not selected previously.

   b. Select the devices from which you want to delete the device image.

      The Select Devices status bar shows the total number of devices that you selected. The status bar is dynamically updated as you select the devices.

   c. To select all devices, select the check box in the column header next to Device Name.

   To select devices on the basis of tags:

   a. Click the **Select by Tags** option.

      The Select by tags list is activated.

   b. Click the arrow on the **Select by Tags** list.

      A list of tags defined for devices in the Junos Space system appears, categorized into two—Public and Private.

c. To select tags, perform one of the following actions :

- Select the check boxes next to the tag names to select the desired tags and click **OK**.
- To search for a specific tag, enter the first few letters of the tag name in the **Select by Tags** field to the left of the **OK** button. If a match is found, a suggestion is made. You can select the suggested tag name and click **OK**.

As you select the tags, the total number of devices associated with the selected tags appears just above the device display table. For example, if there are six devices associated with the selected tags, then **6 items selected** is displayed. However, no devices are listed if the image is not staged on the devices that are associated with the selected tags.

The selected tags appear next to the **Tags Selected** label. An [X] icon appears after each tag name. You can use the [X] icon to clear any tag from the list. The device count decrements accordingly.

From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.

To select devices using a CSV file:

a. Select the **Select by CSV** option.

b. Click **Browse** and upload the file in CSV format containing the list of devices from which you want to remove the device image.

> **TIP:** For a sample CSV file, click the **Sample CSV** link. You are prompted to save the file. Save the file to your local system and open it by using an application such as Microsoft Excel.

From Release 16.1R2 onward, when you upload a CSV file to select devices from, Junos Space Platform verifies the devices in the CSV file. If the CSV file contains devices to which the changes do not apply, a warning message appears which says **Few devices are not selected due to precondition failure. Please click "View inapplicable devices" for more details.**

You can click the **View inapplicable devices** link to review the list of devices that are excluded from the update. The reason for exclusion is listed as an error message against each device.

5. (Optional) Schedule the delete operation by performing one of the following actions.

- Select the **Schedule at a later time** check box and specify a later start date and time for the delete operation.

- Clear the **Schedule at a later time** check box (the default) to initiate the delete operation as soon as you click Remove.

6. Click **Remove**.

> **NOTE:**
> - When you delete the jinstall image, the corresponding jbundle image, if any, is also deleted from the **/var/tmp** folder on the device.
> - On devices with dual Routing Engines, the image is deleted from both Routing Engines. That is, if the image is deleted from the primary Routing Engine, then the image is deleted from the backup Routing Engine as well.

The image is deleted from the selected devices and a message appears, displaying the job ID. To verify whether the image is deleted successfully, click the *job ID* link or navigate to the Job Management page and view the status of the job. If the job is a failure, you can double-click the row corresponding to the job to view the reason for failure. The Job Details page appears, which displays the reason for failure in the **Description** column. If there is an error, the View Job Details page displays an error message. For more information about the error messages, see "Common Error Messages in Device-Related Operations" on page 992.

When you delete a device image from a device, an audit log entry is automatically generated.

Release History Table

Release	Description
17.2	From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.

RELATED DOCUMENTATION

Device Images Overview | **613**

Deleting Device Images | **671**

Viewing Device Association of Images | **659**

Deleting Device Images

Using Junos Space Network Management Platform, you can delete device images from the Junos Space server.

> **NOTE:** You can delete satellite software packages and Junos Continuity software packages from the Junos Space server by following the procedure for deleting device images.

To delete device images from the Junos Space server:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Images**.

   The Images page appears.

2. Select the images that you want to delete.

   The selected images are highlighted.

3. Click the **Delete Device Images** icon.

   If any of the selected device images is associated with a device, a warning message is displayed. You must remove the device images from the devices on which they are staged before you can delete them from the Junos Space server. If none of the device images is associated with any device, the Delete Device Image dialog box appears and displays the image filename and the image version number. This dialog box might display a warning in scenarios where the image you are trying to delete is being staged or deployed on to devices.

4. Click **Delete** to confirm deletion.

   The selected images are deleted from Junos Space Platform and are no longer visible on the Images page.

RELATED DOCUMENTATION

- Removing Device Images from Devices | 666
- Device Images Overview | 613
- Deploying Device Images | 637
- Staging Device Images | 620

CHAPTER 37

Managing Scripts

IN THIS CHAPTER

- Scripts Overview | **673**
- Promoting Scripts Overview | **676**
- Importing Scripts to Junos Space | **676**
- Viewing Script Details | **681**
- Modifying Scripts | **684**
- Modifying Script Types | **687**
- Comparing Script Versions | **688**
- Staging Scripts on Devices | **689**
- Verifying the Checksum of Scripts on Devices | **693**
- Viewing Verification Results | **695**
- Enabling Scripts on Devices | **696**
- Executing Scripts on Devices | **700**
- Executing Scripts on Devices Locally with JUISE | **704**
- Viewing Execution Results | **708**
- Exporting Scripts in .tar Format | **709**
- Viewing Device Association of Scripts | **710**
- Marking and Unmarking Scripts as Favorite | **711**
- Disabling Scripts on Devices | **713**
- Removing Scripts from Devices | **716**
- Deleting Scripts | **720**
- Script Annotations | **721**
- Script Example | **727**

Scripts Overview

Scripts are configuration and diagnostic automation tools provided by the Junos operating system (Junos OS). They help reduce network downtime and configuration complexity, automate common tasks, and reduce the time required to resolve problems. Junos OS scripts are of three types: commit, op, and event scripts.

- Commit scripts—Commit scripts enforce custom configuration rules and can be used to automate configuration tasks, enforce consistency, prevent common mistakes, and more. Every time a new candidate configuration is committed, the active commit scripts are called to inspect the new candidate configuration. If a configuration violates your custom rules, the script can instruct the Junos OS to perform various actions, including making changes to the configuration and generating custom, warning, and system log messages.
- Operation (Op) scripts—Op scripts enable you to add your own commands to the operational mode CLI. They can automate the troubleshooting of known network problems and correct them.
- Event scripts—Event scripts use event policies to enable you to automate network troubleshooting by diagnosing and fixing issues, monitoring the overall status of the router, and examining errors periodically. Event scripts are similar to op scripts but are triggered by events that occur on the device.

Using Junos Space Network Management Platform, you can import multiple scripts into the Junos Space server. You can then perform tasks such as modifying the scripts, viewing their details, exporting their contents, comparing the contents, viewing their association with devices, and staging them on multiple devices simultaneously. After you stage scripts on devices, you can use Junos Space Platform to enable, disable, or execute the scripts on those devices. You can remove the scripts from the devices as well. To help ensure that the staged scripts are not corrupt, you can verify the checksum of the scripts.

Junos Space Platform also supports task scheduling. You can specify the date and time at which you want a script to be staged, verified, enabled, disabled, removed, or executed.

Junos Space Platform associates scripts with devices when you stage scripts on the devices. As part of this association, Junos Space Platform maintains information pertaining to the current status of the script on the device. Based on this feature, Junos Space Platform supports the following operations:

- Associating scripts with devices and maintaining the association
- Displaying the status (version, enabled, or disabled) of scripts on the devices
- Displaying the results of script execution on the devices
- Upgrading the scripts to the latest version on some or all associated devices
- Upgrading the staged script on the associated devices whenever the script is modified from Junos Space Platform
- Marking and unmarking scripts as favorites
- Removing the script-device association

NOTE:

- You can perform script-related operations on a device (enable, disable, remove, verify, or execute scripts— but you cannot stage scripts) only if the scripts are associated with the device.
- If you want to delete scripts from Junos Space Platform, first remove the scripts from the device (using the Remove Scripts from Devices action) and then delete all the related associations.
- You cannot modify the script type if the script is associated with a device. You need to first remove the scripts from the device and then modify the script type.

Based on the roles assigned to your username, Junos Space Platform enables or disables different tasks. You can enable and disable scripts on devices only if you are a Super Administrator with all permissions or a user who has been given maintenance privileges.

For more information about the roles that you need to be assigned to perform any tasks on scripts, see "Predefined Roles Overview" on page 999.

NOTE: The Junos OS management process executes commit scripts with root permissions, not the permission levels of the user who is committing the script. If the user has the permissions required to commit the configuration, then Junos OS performs all actions of the configured commit scripts, regardless of the privileges of the user who is committing the script.

You can perform the following tasks from the Scripts page:

- Import scripts.
- View script details.
- Modify a script.
- Delete scripts.
- Disable scripts on devices.
- Enable scripts on devices.
- Execute a script on devices.
- Remove scripts from devices.
- Stage scripts on devices.
- Compare script versions.
- Export scripts in **.tar** format.

- Modify the type of script.
- View associated devices.
- View verification results.
- Verify the checksum of scripts on devices.
- View execution results.
- Assign scripts to domains.
- Tag and untag the scripts, view the scripts that are tagged, and delete private tags.

To run any of your scripts on devices, see "Executing Scripts on Devices" on page 700 and "Executing Scripts on Devices Locally with JUISE" on page 704.

RELATED DOCUMENTATION

Device Images and Scripts Overview | **609**

Promoting Scripts Overview | **676**

Importing Scripts to Junos Space | **676**

Viewing Script Details | **681**

Modifying Scripts | **684**

Staging Scripts on Devices | **689**

Enabling Scripts on Devices | **696**

Executing Scripts on Devices | **700**

Deleting Scripts | **720**

Promoting Scripts Overview

The promote script feature of Junos Space Network Management Platform enables you to execute a script as an action from the shortcut menu. This feature is an alternative option to executing Scripts from the Execute Scripts window. You can promote scripts to create actions for devices, physical interfaces, logical interfaces, and physical inventory components.

With script promotion, the script execution task is available as a right-click action. You can select the device and execute the script directly. In the absence of the promote scripts feature, to execute a script on a device, you must select the device on the Device Management page and select **Device Operations** > **Execute Scripts** from the Actions menu. You must then select the required script from the Execute Scripts window, provide parameters, and then execute the script.

To promote scripts, include the @PROMOTE annotation with the value set to *yes*. /*@PROMOTE=”yes”*/

Device scripts that are not staged and enabled appear as disabled in the right-click action menu. In the case of device scripts, if the promoted script is not staged and enabled, it will appear as a disabled action. But for interfaces and physical inventory components, the promoted script does not appear on the menu at all if it is not staged and enabled.

Local scripts can also be promoted and are not subject to these restrictions.

> **NOTE:** The promote script feature works only when the option “Advanced Xpath Processing” is enabled. You can enable this option from **Administration > Applications > Modify Application Settings > CLIConfiglets**. Only operation scripts can be promoted. You can promote up to 25 scripts, but you cannot execute multiple promoted scripts simultaneously.

RELATED DOCUMENTATION

Scripts Overview | 673

Importing Scripts to Junos Space

IN THIS SECTION

- Importing Scripts from Files | 677
- Importing Scripts from a Git Repository | 678

Using Junos Space Network Management Platform, you can import a single script or multiple scripts at a time to the Junos Space server from the Scripts page of the Images and Scripts workspace. Junos Space Platform enables you to import commit, operation (op), or event scripts in the **.slax** or **.xsl** format from your computer or from an external Git repository.

Prior to Junos OS 9.0, event scripts and op scripts are saved in the op directory and enabled under the system scripts op hierarchy. However, from Junos OS 9.0 onward, event scripts are saved in the event directory and enabled under the event-options event-script hierarchy.

> **NOTE:** If you want to import multiple scripts at a time, use the Mozilla Firefox or Google Chrome Web browser. Currently, Internet Explorer does not support the selection of multiple files. In addition, note that two scripts with the same name cannot be imported into the Junos Space server.

Junos Space Platform provides the following options to import scripts:

Importing Scripts from Files

You can import scripts in the **.slax** or **.xsl** format from your computer by using the **Import from files** option on the Import Scripts page. Starting with Junos Space Network Management Platform Release 15.2R1, multiple scripts can also be imported to the Junos Space server as **.tar** files.

To import scripts from files:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Scripts**.

   The Scripts page appears.

2. Click the **Import Script** icon.

   The Import Scripts page appears.

3. Select **Import from files**, if the option is not already selected.

4. Click **Browse**.

   The File Upload dialog box displays the directories and folders on your local file system.

5. Select the file or files that you want to import and click **Open**.

   The selected filenames appear in the box beside the Browse button.

6. Click **Next**.

If the selected scripts are valid, they are displayed on the Import Scripts page.

NOTE:

- If the selected scripts are not valid, an error message is displayed. Click **OK** to return to the Import Scripts page.
- If some of the scripts are valid and others are not, a warning message indicating that some of the scripts are not valid is displayed. Click **OK** to import the valid scripts.

  To determine which scripts are imported and which are not, view the job details from the Job Management page.
- If you have selected multiple scripts of the same name, an error message indicating the presence of duplicate scripts is displayed and the duplicate scripts are not imported.

Details of the scripts selected for import, such as information about whether the scripts already exist in Junos Space Platform and whether conflicts exist, are displayed in a tabular format. Table 82 describes the fields displayed on the page.

7. (Optional) Select the **Exclude Conflicting Scripts From Import** check box to select only those scripts for which there are no conflicts with the script versions that exist in Junos Space Platform.

   The scripts for which conflicts exist are removed from the list of scripts on the Import Scripts page.

8. Click **Finish** to import the listed scripts or click **Cancel** to go back to the Scripts page.

   If you have not selected the Exclude Conflicting Scripts From Import check box and the script files already exist in Junos Space Platform, a warning message indicating that conflicts exist and that the scripts will be overwritten is displayed. Click **OK** to proceed with the import or click **Cancel** to return to the Import Scripts page.

   The scripts are imported to the domain that you are currently logged in to. If a script with the same name already exists in the domain or any of the subdomains, and you choose to override any conflicts that might exist, the script is imported to the domain and subdomains where the script exists, with the version number incremented. This ensures that the script that exists in Junos Space is not overwritten and can be retrieved if required.

   The imported scripts are displayed on the Scripts page.

Importing Scripts from a Git Repository

You can import scripts in the **.slax** or **.xsl** format from external Git repositories. Before you import scripts from a Git repository, the repository must be added to Junos Space and marked as the active Git repository for scripts, from the Git Repositories page. When you import scripts from Git repositories, all scripts in the selected branch of the repository are imported to Junos Space.

To import scripts from a Git repository:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Scripts**.

   The Scripts page appears.

2. Click the **Import Script** icon.

   The Import Scripts page appears.

3. Select **Import from Git**.

   This option is displayed only if an active Git repository of the Scripts type exists in Junos Space.

4. Select the branch of the repository from the **Git Branch** list.

5. (Optional) Click **Sync Now** to synchronize the Git repository clone on the Junos Space server with the external Git repository.

   The date and time of the last sync is displayed above the Sync Now button.

6. Click **Next**.

   If the scripts in the selected Git repository branch are valid, they are displayed on the Import Scripts page.

   NOTE:
   - If the selected scripts are not valid, an error message is displayed. Click **OK** to return to the Import Scripts page.
   - If some of the scripts are valid and others are not, a warning message indicating that some of the scripts are not valid is displayed. Click **OK** to import the valid scripts.

     To determine which scripts are imported and which are not, view the job details from the Job Management page.
   - If you have selected multiple scripts of the same name, an error message indicating the presence of duplicate scripts is displayed and the duplicate scripts are not imported.

   Details of the scripts selected for import, such as information about whether the scripts already exist in Junos Space Platform and whether conflicts exist, are displayed in a tabular format. Table 82 describes the fields displayed on the page.

7. (Optional) Select the **Exclude Conflicting Scripts From Import** check box to import only those scripts for which there are no conflicts with the script versions that exist in Junos Space Platform.

The scripts for which conflicts exist are removed from the list of scripts on the Import Scripts page.

8. Click **Finish** to import the listed scripts or click **Cancel** to go back to the Scripts page.

   If you have not selected the Exclude Conflicting Scripts From Import check box and conflicts exist, a warning message indicating that conflicts exist and that the scripts will be overwritten is displayed. Click **OK** to proceed with the import or click **Cancel** to return to the Import Scripts page.

   The scripts are imported to the domain that you are currently logged in to. If a script with the same name already exists in the domain or any of the subdomains, and you choose to override any conflicts that might exist, the script is imported to the domain and subdomains where the script exists, with the version number incremented. This ensures that the script that exists in Junos Space is not overwritten and can be retrieved if required.

   The imported scripts are displayed on the Scripts page.

Table 82: Import Scripts Page Fields

Fields	Description
Script	Name of the script
Conflict State	Whether a conflict exists between the selected script and a script with the same name in Junos Space Platform. Value can be NEW, NO CONFLICT, or CONFLICT. **NOTE:** When scripts are imported using the Import from File option, the two possible states are NEW and CONFLICT. If the script does not exist in Junos Space Platform, the state is NEW; if a script of the same name exists in Junos Space Platform, the state is CONFLICT. Value is NEW when the script is imported to Junos Space Platform for the first time. Value is NO CONFLICT when there is no conflict between the script selected for import from the Git repository and the scripts that exist in Junos Space Platform. Value is CONFLICT when: • You are importing scripts from your computer and a script of the same name exists in Junos Space Platform. • A script of the same name exists in Junos Space Platform and the script is being imported for the first time from the Git repository. • The selected script is already imported from the Git repository and is modified in Junos Space Platform. • The script present in Junos Space Platform is from a different branch of the Git repository.
Domain	Domain to which the existing script in Junos Space Platform is assigned The column is empty if the script does not exist in Junos Space Platform.

Table 82: Import Scripts Page Fields *(continued)*

Fields	Description
Latest Version	Latest version of the script in Junos Space Platform The column is empty if the script does not exist in Junos Space Platform.
Git Version	Commit ID of the script that was previously imported to Junos Space Platform. A warning icon is displayed if the script was later modified in Junos Space Platform. The column is empty if the script does not exist in Junos Space Platform or if no version of the script in Junos Space Platform is imported from a Git repository.
Git Branch	Git repository branch from which the existing script was last imported The column is empty if the script does not exist in Junos Space Platform or if no version of the script in Junos Space Platform is imported from a Git repository.
Last Commit	Commit ID of the last commit of the script in the selected branch of the Git repository The column is empty if the script is being imported from your computer.

Release History Table

Release	Description
15.2R1	Starting with Junos Space Network Management Platform Release 15.2R1, multiple scripts can also be imported to the Junos Space server as **.tar** files.

RELATED DOCUMENTATION

Viewing Script Details | **681**

Git Repositories in Junos Space Overview | **1485**

Viewing Script Details

The Images and Scripts workspace enables you to view and manage multiple scripts in Junos Space Network Management Platform. You can view information about scripts that are stored in the Junos Space Platform database from the Scripts page. To view detailed information about a particular script, you can use the View Script Details option.

To view scripts from the Scripts page:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Scripts**.

   The Scripts page appears, displaying the scripts that you imported into Junos Space Platform.

   Table 83 describes the fields displayed on the Scripts page.

   You can use the filter option on the **Script Name**, **Domain**, **Descriptive Name**, **Type**, **Category**, **Execution Type**, **Format**, and **Latest Revision** drop-down lists to specify the filter criteria. When you apply the filters, the table displays only the scripts that match the filter criteria. The **Description**, **Creation Date**, **Last Updated Time**, and **Associations** fields do not support the filter option.

2. Select a script and click the **View Script Details** icon, or double-click the script whose details you want to view.

   The **Script Details** dialog box displays the script name, type, format, creation time, version, script contents, and comments. By default, the latest version of the script is displayed. Use the scroll bar to the right of the page to scroll through the script.

   Table 84 describes the fields displayed on the Script Details dialog box.

Table 83: Fields on the Scripts Page

Field	Description
Script Name	Name of the script file
Domain	Domain to which the script belongs
Descriptive Name	Descriptive name of the script
Type	Type of script can be one of the following: • Commit Script • Op Script • Event Script
Category	Category of the script
Execution Type	• Device—Scripts of this type need to be staged and enabled on a device before the scripts can be executed. • Local—Scripts of this type need not be staged or enabled on a device for the scripts to be executed. You must set the @ISLOCAL annotation to true to execute the script locally. For more information about script annotations and a sample script, see "Script Annotations" on page 721 and "Script Example" on page 727.

Table 83: Fields on the Scripts Page *(continued)*

Field	Description
Format	Format of the script file can be one of the following: • XSL • SLAX
Latest Revision	Latest revision number of the script in Junos Space Platform
Git Version	Commit ID of the script in the Git repository when it is imported. If the script is modified in Junos Space Platform after import, a Warning icon is displayed alongside. If the script is not imported from a Git repository, the value displayed is **N/A**.
Git Branch	Git repository branch from which the script is imported. If the script is not imported from a Git repository, the value displayed is **N/A**.
Creation Date	Date and time when the script was imported to the Junos Space server
Description	Description of the script
Last Updated Time	Time when the script was last updated
Associations	**View** link to view device associations

Table 84: Script Details Dialog Box Fields

Field	Description
Name	Name of the script file
Type	Type of script. The values can be one of the following: • Commit script • Op script • Event script
Format	Format of the script file. The values can be one of the following: • XSL • SLAX
Creation Time	Date and time when the script was created
Version	Version number of the script. When you modify a script, the changes are saved as the latest version of the script.

Table 84: Script Details Dialog Box Fields *(continued)*

Field	Description
Script contents	Contents of the script
Comments	Text that describes the script that is entered by the user

RELATED DOCUMENTATION

Scripts Overview | 673

Exporting Scripts in .tar Format | 709

Modifying Scripts

You can use Junos Space Network Management Platform to modify the script type, script contents, and the script version. You can also add your comments describing the script. When you modify a script, the script is saved as the latest version by default. Junos Space Platform modifies both associated and unassociated scripts.To modify the script type for multiple scripts, see "Modifying Script Types" on page 687.

You can modify and save a script to the Junos Space Platform database without staging the modified (or the latest) script on the devices. When you do not stage the latest version, the older script continues to exist on the devices on which it was previously staged. To both save and stage the modified script, use the **Save & Stage** action instead of **Save & Exit** action while modifying the script.

To modify a script:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Scripts**.

   The Scripts page displays the scripts that you imported into Junos Space Platform.

2. Select the script that you want to modify.
3. Select **Modify Script** from the shortcut menu or click the **Modify Script** icon.

   The **Modify Script** page displays the details of the script.

4. You can modify the script type, version, script contents, and the comments about the script. You cannot modify the script type if the script is associated with any device.

   If you have multiple versions of the script, select the correct version of the script from the **Version** list to modify the script. By default, the latest version of the script is displayed. The changes that you make are saved as the latest version of the script.

5. Perform one of the following tasks:

- Click **Cancel** if you do not want to make any changes to the script.

  You are returned to the Scripts page.

- Click **Save & Exit** to save the changes to the script and exit the Modify Script page. The script is saved as the latest version in the Junos Space database.

  You are returned to the Scripts page.

- Click **Save & Stage** to save the changes to the script as the latest version in the Junos Space database and to stage the latest version of the script on devices.

  The Stage Script on Device(s) page appears, displaying a list of all the associated devices.

  > **TIP:** If you do not see any device listed, it means that no previous version of the script is associated with any of the devices. First, stage the script by using the **Stage Scripts on Devices** task from the Actions menu, and then modify and stage the modified script by using the **Modify Script** task.

  To stage the modified script:

  1. On the **Stage Scripts on Device(s)** page, select the devices on which you want the modified script to be staged, by using one of the following selection modes—manually or on the basis of tags.These options are mutually exclusive. If you select one, the other is disabled.

     > **NOTE:** By default, the **Select by Device** option is selected and the complete list of devices is displayed. If you have tagged any of the devices and you want only those tagged devices with which the scripts are associated to be displayed, choose the **Select by tags** option.

     - To select devices manually:
       - Click the **Select by Device** option and select the devices on which you want to stage the modified script. The Select Devices status bar shows the total number of devices that you have selected; the status bar is dynamically updated as you select the devices.
       - To select all the devices, select the check box in the column header next to Host Name.
     - To select devices on the basis of tags:
       - Click the **Select by Tags** option. The Select by tags list is activated.
       - Click the arrow on the **Select by Tags** list. A list of tags defined on devices in Junos Space Platform appears, displaying two categories of tags—Public and Private.

To select tags, perform one of the following actions :

- Select the check boxes next to the tag names to select the desired tags and click **OK**.
- To search for a specific tag, enter the first few letters of the tag name in the **Select by Tags** field to the left of the **OK** button. If a match is found, a suggestion is made. Select the suggested match and click **OK**.

The total number of devices associated with the selected tags appears in the **Select Devices** status bar above the options.

The selected tags appear in the status bar below the option buttons, next to the **Tags Selected** label. An [X] icon appears after each tag name. You can use the [X] icon to clear any tag from the list. The device count in the Select Devices status bar decrements accordingly. The table below this status bar displays the selected devices.

2. (Optional) To schedule a time for staging the script, select the **Schedule at a later time** check box and specify the date and time when you want the script to be staged.

3. Click **OK** on the Stage Script on Device(s) page.

   You are returned to the Scripts page. If the modification of the script is successful, the **Latest Revision** column on this page displays the latest and updated script version number.

6. (Optional) To verify the changes made, you can view the details of the script. See "Viewing Script Details" on page 681.

   The **Latest Version** column displays the latest version.

7. Click **Cancel** to withdraw your changes and return to the **Scripts** page.

For troubleshooting, see the following log: **/var/log/jboss/server.log**. No audit logs are generated for this task.

To verify whether the latest script version is successfully staged on devices:

1. On the Scripts page, select the script (if it is not selected).

   Typically, the script remains selected on the Scripts page when you are returned to this page after the modification of the script.

2. Select **View Associated Devices** from the Actions menu.

   The View Associated Device page appears. If the staging is successful, then the version numbers on the **Latest Version** and **Staged Version** columns must match.

   To return to the Scripts page, click **Scripts** on the breadcrumb.

RELATED DOCUMENTATION

Staging Scripts on Devices | 689
Scripts Overview | 673
Modifying Script Types | 687
Comparing Script Versions | 688

Modifying Script Types

Using Junos Space Network Management Platform, you can modify the script type of multiple scripts simultaneously.

To modify the script type:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Scripts**.

   The Scripts page displays the scripts that you imported into Junos Space Platform.

2. Select the script whose script type you want to modify.

3. Select **Modify Scripts Type** from the Actions menu. This action is unavailable if the selected script is associated with any device.
   The **Modify Scripts Type** dialog box displays the details of the script.

4. Use the **Bulk Actions** list to select a common script type for all scripts. To modify script types of individual scripts, click the value list in the **Script Type** column heading to make your changes.

5. Click **Apply**.
   Your changes are saved and the Scripts page appears.

6. (Optional) To verify, double-click the script that you modified and view the script type.

RELATED DOCUMENTATION

Viewing Script Details | 681
Staging Scripts on Devices | 689

Comparing Script Versions

Using Junos Space Network Management Platform, you can compare two scripts and view their differences. This comparison can be done with two different scripts or between different versions of the same script.

To compare scripts:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Scripts**.

   The Scripts page displays the scripts that you imported into Junos Space Platform.

2. Select the script that you want to compare.

3. Select **Compare Script Versions** from the Actions menu.

   The **Compare Scripts** dialog box appears.

4. Use the **Source script** and **Target script** lists to select the scripts that you want to compare.

5. Use the **Version** lists to specify the versions of the source and target scripts that you want to compare.

6. Click **Compare.**

   The differences between the scripts are displayed in the **View Diff** dialog box. Use the **Next Diff** and **Prev Diff** buttons to navigate to the next change or the previous change, respectively.

   The differences between the two scripts are represented using three different colors:

   - Green—The green text represents the contents that appear only in the source script.
   - Blue—The blue text represents the contents that appear only in the target script.
   - Purple—The purple text represents the contents that are different between the two scripts.

   Next to the **Next Diff** and **Prev Diff** buttons, the total number of differences, the number of differences in the source script, the number of differences in the target script, and the number of changes are displayed.

7. Click **Close** to close the window and return to the Compare Scripts page.

RELATED DOCUMENTATION

Modifying Scripts | 684

Staging Scripts on Devices | 689

Scripts Overview | 673

Staging Scripts on Devices

Junos Space Network Management Platform enables you to stage a single script or multiple scripts on one device or multiple devices simultaneously. Staging a script enables you to hold a script on a device, ready to be executed when required. When you select scripts that are previously staged on one or more devices from the Scripts page, then the GUI lists only the devices that are not associated with any of the selected scripts and the devices with older versions of the selected scripts. This listing of the devices allows you to associate scripts with new devices and also upgrade scripts to the latest version on already associated devices.

To stage a script on devices:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Scripts**.

   The Scripts page appears.

2. Select the scripts that you want to stage on one or more devices. The selected scripts are highlighted.

3. Select **Stage Scripts on Devices** from the Actions menu.

   The Stage Scripts on Device(s) page appears, displaying:

   - A list of the selected scripts and the latest versions of the scripts. By default, the latest version of the script is staged on the selected devices. However, to stage a previous version of the script, select the suitable version from the drop-down list below the **Version** column.
   - A list of the Junos Space Platform devices that are not associated with any of the selected scripts and also the devices with the older versions of the selected scripts.

4. (Optional) Keep the **Enable Scripts on Devices** check box selected if you want the scripts to be enabled and ready to be executed when you stage them on devices from Junos Space Platform. Clear this check box if you want the scripts to be disabled on the devices.

5. (Optional) To include the devices on which the selected scripts are already staged , select the **Show existing Staged Devices** check box. The device list is updated to include devices on which the script is already staged.

6. Select the devices to stage the selected script.

   You can select devices by using one of the following selection modes—manually, on the basis of tags, or by using a comma-separated values (CSV) file. These options are mutually exclusive. If you select one, the others are disabled.

> **NOTE:** By default, the **Select Device Manually** option is selected and the list of devices that are not associated with any of the selected scripts and devices with the older versions of the selected scripts is displayed.

- To select devices manually:
  - Click the **Select Device Manually** option and select the devices on which you want to stage the script. The Select Devices status bar shows the total number of devices that you selected; the status bar is dynamically updated as you select the devices.
  - To select all devices, select the check box in the column header next to the Host Name column.
- To select devices on the basis of tags:

  a. Click the **Select by Tags** option. The Select by tags list is activated.

  b. Click the arrow on the **Select by Tags** list. A list of tags defined on devices in the Junos Space system appears, displaying two categories of tags—Public and Private.

  > **NOTE:** No tag is displayed if none of the devices is associated with any tag. You need to tag the devices on the Device Management page before you can use the **Select by Tags** option.

  c. To select tags, perform one of the following actions:
     - Select the check boxes next to the tag names to select the desired tags and click **OK**.
     - To search for a specific tag, enter the first few letters of the tag name in the **Select by Tags** field to the left of the **OK** button. If a match is found, a suggestion is made. Select the suggested match and click **OK**.

     As you select the tags, the total number of devices associated with the selected tags appears just above the device display table. For example, if there are six devices associated with the selected tags, then **6 items selected** is displayed.

     The selected tags appear next to the **Tags Selected** label. An [X] icon appears after each tag name. You can click the [X] icon to clear any tag from the list. The device count decrements accordingly.

     The device display table displays the devices associated with the selected tags.

- From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.

To select devices by using a CSV file:

a. Select the **Select by CSV** option.

b. Click **Browse** to navigate to the file location on your computer and select the CSV file containing the list of devices on which you want to stage the script.

> **TIP:** For a sample CSV file, click the **Sample CSV** link. You are prompted to save the file. Save the file to your computer and open it by using an application such as Microsoft Excel.

c. Click **Upload** to upload the CSV file.

From Release 16.1R2 onward, when you upload a CSV file to select devices from, Junos Space Platform verifies the devices in the CSV file. If the CSV file contains devices to which the changes do not apply, a warning message appears which says **Few devices are not selected due to precondition failure. Please click "View inapplicable devices" for more details.**

You can click the **View inapplicable devices** link to review the list of devices that are excluded from the update. The reason for exclusion is listed as an error message against each device.

- From Junos Space Platform Release 18.2R1 onward, you can select devices based on saved filters

To select devices by using a saved filter:

a. Select the **Select by Filter** option.

b. Select the filter from the list of saved filters.

The devices associated with the selected filter appears in the grid.

7. (Optional) To schedule a time for staging the script, select the **Schedule at a later time** check box and use the calendar icon and drop-down list to specify the date and time, respectively, when you want the script to be staged.

8. Click **Stage**. The script is staged on the selected device or devices. The Stage Scripts Information page displays the job ID.

9. Perform one of the following actions on the Stage Scripts Information page:

- To verify the status of this job, click the ***job ID*** in this page.

The Job Management page appears. Double-click the row corresponding to the staging job. The Script Management Job Status page appears and the **Description** column on this page displays whether

or not the script is staged successfully and reasons for failure (if staging of the script failed). If Junos Space Platform detects an SSH fingerprint mismatch between the one on the device and that in the Junos Space Platform database, the connection is dropped. The Connection Status displays Down and Authentication Status displays Fingerprint Conflict on the Device Management page. The View Job Details page displays an error message. For more information about the error messages and solutions, see "Common Error Messages in Device-Related Operations" on page 992.

- Click **OK** to go back to the Scripts page.

On the Scripts page, click **View** in the **Associations** column of that staged script to view the details of the Script - Device association. For more information about viewing the device associations for scripts, see "Viewing Device Association of Scripts" on page 710.

On the Job Management page, you can export details about staging of a script as a CSV file to your local file system:

1. On the Junos Space Platform UI, select **Jobs** > **Job Management**.

   The Job Management page appears.

2. Double-click the row corresponding to the staging job.

   The Script Management Job Status page appears.

3. Click **Export as CSV**.

   You are prompted to save the file.

4. Click **OK** on the File Save page to save the file to your local file system.

5. After you save the file, to return to the Job Management page, click **OK** on the **Exporting Script Job** page.

   Use an application such as Microsoft Excel to open the downloaded file from your local system.

On the left pane of the UI, select **Images and Scripts** > **Scripts** to return to the Scripts page.

Release History Table

Release	Description
18.2	From Junos Space Platform Release 18.2R1 onward, you can select devices based on saved filters
17.2	From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.

RELATED DOCUMENTATION

Scripts Overview | 673

Viewing Device Association of Scripts | 710

Verifying the Checksum of Scripts on Devices | 693

Executing Scripts on Devices | 700

Verifying the Checksum of Scripts on Devices

When you stage a script on a device using Junos Space Network Management Platform, it is possible that the script might not be completely transferred to the device. Verifying the checksum helps validate that the script has been staged properly. Junos Space Platform enables you to verify the checksum of multiple scripts that are staged on the devices.

When you verify scripts that have multiple versions, the latest versions of selected scripts are verified with the versions of the scripts that are available on the device. If the version of the script present on the device does not match the version that it is compared with, Junos Space Platform displays an error message.

To verify the checksum of a script:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Scripts**.

   The Scripts page displays the scripts that you imported into Junos Space Platform.

2. Select the script or scripts whose checksum you want to verify.
3. From the Actions menu, select **Verify Scripts on Devices**.

   The Verify Checksum of Scripts on Device(s) dialog box appears.

4. Select the devices that have the script staged on them, by using one of the following selection modes—manually, on the basis of tags, or by using the comma-separated values (CSV) file. These options are mutually exclusive. If you select one, the others are disabled.

   NOTE: By default, the **Select by Device** option is selected and the list of devices that can be selected is displayed.

   - To select devices manually:
     - Click the **Select by Device** option and select the devices that have the script staged on them. The Select Devices status bar shows the total number of devices that you selected; the status bar is dynamically updated as you select the devices.
     - To select all the devices, select the check box in the column header next to Host Name.

- To select devices on the basis of tags:

  1. Click the **Select by Tags** option. The Select by tags list is activated.

  2. Click the arrow on the **Select by Tags** list. A list of tags defined on devices in the Junos Space system appears, displaying two categories of tags—Public and Private.

  3. To select tags, perform one of the following actions :

     - Select the check boxes next to the tag names to select the desired tags and click **OK**.
     - To search for a specific tag, enter the first few letters of the tag name in the **Select by Tags** field to the left of the **OK** button. If a match is found, a suggestion is made. Select the suggested match and click **OK**.

     As you select the tags, the total number of devices associated with the selected tags appears just above the device display table. For example, if there are six devices associated with the selected tags, then **6 items selected** is displayed.

     The selected tags appear next to the **Tags Selected** label. An [X] icon appears after each tag name. You can click the [X] icon to clear any tag from the list. The device count decrements accordingly.

     The device display table displays the devices associated with the selected tags.

- To select devices by using a CSV file:

  1. Select the **Select by CSV** option.

  2. Click **Browse** to navigate to the file location on your computer and select the CSV file containing the list of devices on which you want to verify the script.

     TIP: For a sample CSV file, click the **Sample CSV** link. You are prompted to save the file. Save the file to your computer and open it by using an application such as Microsoft Excel.

  3. Click **Upload** to upload the CSV file.

     From Release 16.1R2 onward, when you upload a CSV file to select devices from, Junos Space Platform verifies the devices in the CSV file. If the CSV file contains devices to which the changes do not apply, a warning message appears which says "Few devices are not selected due to precondition failure. Please click "View inapplicable devices" for more details." You can click the **View inapplicable devices** link to review the list of devices that are excluded from the update.

5. (Optional) To schedule a time for verification, select the **Schedule at a later time** check box and use the calendar icon and drop-down list respectively to specify the date and time when you want the script to be verified.
6. Click **Verify Checksum**.

   The Verify Scripts Information dialog box appears displaying the message that the verification of the script is successfully scheduled and a job ID link.
7. Perform one of the following actions:
   - Click the ***job ID*** link to view the status of the verification operation on the Job Management page.
   - Click **OK** to return to the Scripts page.

For more information about viewing the checksum verification results, see "Viewing Verification Results" on page 695.

RELATED DOCUMENTATION

Enabling Scripts on Devices | **696**

Viewing Verification Results

You can use Junos Space Network Management Platform to make sure that the scripts staged on devices are not corrupted, by verifying the checksum of the scripts. You can also view the results of the checksum verification task. When a verification failure occurs, the results indicate the reason for the failure.

For more information about verifying the checksum of a script, see "Verifying the Checksum of Scripts on Devices" on page 693.

To view the verification results:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Scripts**.

   The Scripts page displays the scripts that you imported into Junos Space Platform.
2. Select the script whose verification results you want to view.
3. Right-click your selection or use the Actions menu, and select **Verification Results**.

   This Verification Results option is available only when you select a script staged on a device. The option is unavailable if you select a local script.

   The **Script Verification Results** page displays the results of the checksum verification. If you have not yet verified the script on the devices, the results page is empty.

   Table 85 describes the fields on the Script Verification Results page.

Table 85: Script Verification Results Page Fields

Field Name	Description
Script Name	Filename of the script that is selected for verifying the checksum
Device Name	Name of the device on which the script is verified
Result	Result of the verification. The values could be one of the following: • Success • Failed • Scheduled
Comments	The comment **Script verified successfully**

4. Click **Back** to return to the Scripts page.

RELATED DOCUMENTATION

Executing Scripts on Devices | 700

Enabling Scripts on Devices

After you stage scripts on devices, you can use Junos Space Network Management Platform to enable these scripts on one or more devices simultaneously.

When you enable scripts that use Junos Space Platform, depending on the type of script, an appropriate configuration is added on the device. For example, for a file named bgp-active.slax, the configuration added to the device is as follows:

- For a commit script:
  Example:
  [edit]
  user@host# set system scripts commit file bgp-active.slax
- For an op script:
  Example:
  [edit]
  user@host# set system scripts op file bgp-active.slax
- For an event script:

Example:
[edit]
user@host# set system scripts event file bgp-active.slax

> **CAUTION:** If the filename of the selected script matches that of any script present on the device, then the script on the device is enabled regardless of its contents.

To enable scripts on devices:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Scripts**.

   The Scripts page displays the scripts that you imported into Junos Space Platform.

2. Select one or more scripts that you want to enable on devices.

3. Select **Enable Scripts on Devices** from the Actions menu.

   The Enable Scripts on Device(s) page appears.

   If the selected scripts are already enabled on the devices, then instead of the Enable Scripts on Device(s) page, Junos Space displays the following message:

   Device(s) having all the selected staged script(s) already have them in enabled state.

   > **NOTE:**
   > - This action does not list devices that are not associated with scripts. It also does not list the devices for which the script is in an enabled state already.
   > - If you select multiple scripts, then only those devices that are associated with all the selected scripts are displayed.

4. Select the devices on which you want the script to be enabled, by using one of the following selection modes—manually, on the basis of tags, or by using the comma-separated values (CSV) file. These options are mutually exclusive. If you select one, the others are disabled.

   > **NOTE:** By default, the **Select Device Manually** option is selected and the list of devices that can be selected is displayed.

   - To select devices manually:
     - Click the **Select Device Manually** option and select the devices on which you want to enable the device script. The Select Devices status bar shows the total number of devices that you have selected; the status bar is dynamically updated as you select the devices.
     - To select all the devices, select the check box in the column header next to the Host Name column.

- To select devices on the basis of tags:

  1. Click the **Select by Tags** option. The Select by tags list is activated.

  2. Click the arrow on the **Select by Tags** list. A list of tags defined on devices in the Junos Space system appears, displaying two categories of tags—Public and Private.

     > **NOTE:** If no tags are displayed, then it means that none of the devices is associated with any tag. You need to tag the devices on the Device Management page before you can use the **Select by Tags** option.

  3. To select tags, perform one of the following actions :

     - Select the check boxes next to the tag names to select the desired tags and click **OK**.
     - To search for a specific tag, enter the first few letters of the tag name in the **Select by Tags** field to the left of the **OK** button. If a match is found, a suggestion is made. Select the suggested match and click **OK**.

     As you select the tags, the total number of devices associated with the selected tags appears just above the device display table. For example, if there are six devices associated with the selected tags, then **6 items selected** is displayed.

     The selected tags appear next to the **Tags Selected** label. An [X] icon appears after each tag name. You can click the [X] icon to clear any tag from the list. The device count decrements accordingly.

     The device display table displays the devices associated with the selected tags.

- To select devices by using a CSV file:

  1. Select the **Select by CSV** option.

  2. Click **Browse** to navigate to the file location on your computer and select the CSV file containing the list of devices on which you want to enable the script.

     > **TIP:** For a sample CSV file, click the **Sample CSV** link. You are prompted to save the file. Save the file to your computer and open it by using an application such as Microsoft Excel.

  3. Click **Upload** to upload the CSV file.

     From Release 16.1R2 onward, when you upload a CSV file to select devices from, Junos Space Platform verifies the devices in the CSV file. If the CSV file contains devices to which the changes

do not apply, a warning message appears which says "Few devices are not selected due to precondition failure. Please click "View inapplicable devices" for more details." You can click the **View inapplicable devices** link to review the list of devices that are excluded from the update.

5. (Optional) To schedule a time for enabling the script, select the **Schedule at a later time** check box and use the calendar icon and drop-down list respectively to specify the date and time when you want the script to be enabled.
6. Click **Enable**.

   The selected scripts are enabled on the devices, and the Enable Scripts Information dialog box displays a link to the job ID.

   Perform one of the following actions on the Enable Scripts Information dialog box:

   - Click the ***job ID*** link to view the status of this task on the Job Management page.

     The Job Management page appears. Double-click the job pertaining to the enabling operation. The Script Management Job Status page appears and the **Description** column on this page displays whether or not the script is enabled successfully on the devices and reasons for failure (if enabling of the script had failed). For more information about the error messages, see "Common Error Messages in Device-Related Operations" on page 992.

   - Click **OK** to return to the Scripts page.

On the Job Management page, you can export details about enabling of a script as a CSV file to your local file system:

1. On the Junos Space Platform UI, select **Jobs** > **Job Management**.

   The Job Management page appears.

2. Double-click the job pertaining to the script enabling operation.

   The Script Management Job Status page appears.

3. Click **Export as CSV**.

   You are prompted to save the file.

4. Click **OK** on the File Save dialog box to save the file to your local file system.

5. After you save the file, to return to the Job Management page, click **OK** on the **Exporting Script Job** dialog box.

   Use an application such as Microsoft Excel to open the downloaded file from your local system.

On the left pane of the UI, select **Images and Scripts** > **Scripts** to return to the Scripts page.

RELATED DOCUMENTATION

Executing Scripts on Devices | 700

Executing Scripts on Devices

You can use Junos Space Network Management Platform to trigger the execution of op scripts on one or more devices simultaneously. Commit and event scripts are automatically activated after they are enabled. Commit scripts are triggered every time a commit is called on the device and event scripts are triggered every time an event occurs on the device or at a specific time, if a time is specified.

NOTE: If a script does not require XPath processing, you can execute such scripts on more than 200 devices at a time. Scripts that do not require XPath processing include scripts without device-specific or entity-specific parameters and with /, //, or /device as context.

CAUTION: If the filename of the selected script matches that of any script present on the device, then the script on the device is executed regardless of its contents.

To execute an op script on devices:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Scripts**.

   The Scripts page appears, displaying the scripts that you imported into Junos Space Platform.

2. Select the op script that you want to execute on a device.

3. Select **Execute Script on Devices** from the Actions menu. This option is enabled only when the script is staged.

   The Execute Script on Device(s) page appears. If the selected script is already disabled on the devices, then Junos Space displays the following message instead of the Execute Scripts on Device(s) page: **Disabled script cannot be executed.**

   By default, the Execute Script on Device(s) page lists the devices on which the latest version of the script is staged. If no devices are listed, it means that the latest version of the script is not staged yet. If you have staged the previous versions of the script, select one of the staged versions from the **Version** list. The page displays the list of devices on which this version of the script is staged.

> **NOTE:** To find out which version of the script is staged, select the script and click **View** from the **Associations** column on the Scripts page. The **Staged Version** column displays the version of the script that is staged.

4. Select the devices on which you want the script to be executed, by using one of the following selection modes—manually, on the basis of tags, or by using a comma-separated values (CSV) file. These options are mutually exclusive. If you select one, the others are disabled.

   > **NOTE:** By default, the **Select Device Manually** option is selected and the list of devices that can be selected is displayed.

   - To select devices manually:
     - Click the **Select Device Manually** option and select the device(s) that have the script staged on them. The Select Devices status bar shows the total number of devices that you selected; the status bar is dynamically updated as you select the devices.
     - To select all the devices, select the check box in the column header next to the Host Name column.
   - To select devices on the basis of tags:
     1. Click the **Select by Tags** option. The Select by Tags list is activated.
     2. Click the arrow on the **Select by Tags** list. A list of tags defined on devices in Junos Space Platform appears, displaying two categories of tags—Public and Private.

        > **NOTE:** No tag is displayed if none of the devices is associated with any tag. You need to tag the devices on the Device Management page before you can use the **Select by Tags** option.

     3. To select tags, perform one of the following actions:
        - Select the check boxes next to the names of tags that you want to select and and click **OK**.
        - To search for a specific tag, enter the first few letters of the tag name in the **Select by Tags** field to the left of the **OK** button. Suggestions appear if there are matches for the string you enter. Select the suggested match and click **OK**.

        As you select the tags, the total number of devices associated with the selected tags appears just above the device display table. For example, if there are six devices associated with the selected tags, then **6 items selected** is displayed.

The selected tags appear next to the **Tags Selected** label. An [X] icon appears after each tag name. You can click the [X] icon to clear any tag from the list. The device count is updated accordingly.

The device display table displays the devices associated with the selected tags.

- From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.

  To select devices by using a CSV file:

  1. Select the **Select by CSV** option.

  2. Click **Browse** to navigate to the file location on your computer and select the CSV file containing the list of devices on which you want to execute the script.

     TIP: For a sample CSV file, click the **Sample CSV** link. You are prompted to save the file. Save the file to your computer and open it by using an application such as Microsoft Excel.

  3. Click **Upload** to upload the CSV file.

     From Release 16.1R2 onward, when you upload a CSV file to select devices from, Junos Space Platform verifies the devices in the CSV file. If the CSV file contains devices to which the changes do not apply, the following warning message appears: **Few devices are not selected due to precondition failure. Please click "View inapplicable devices" for more details.**

     Click the **View inapplicable devices** link to review the list of devices that are excluded from the update. The reason for exclusion is listed as an error message against each device.

- From Junos Space Platform Release 18.2R1 onward, you can select devices based on saved filters

  To select devices by using a saved filter:

  1. Select the **Select by Filter** option.

  2. Select the filter from the list of saved filters.

     The devices associated with the selected filter appears in the grid.

5. (Optional) To specify values for script execution parameters, click **Value**.
6. (Optional) To schedule a time to execute the script, select the **Schedule at a later time** check box and use the calendar icon and drop-down list to specify the date and time, when you want the script to be executed, respectively.

7. Click **Execute**.

   The selected scripts are executed on the devices, and the Execute Script Information page displays a link to the job ID.

8. Perform one of the following actions on the Execute Scripts Information page:

   - To verify the status of this job, click the ***job ID*** on this page.

     The Job Management page appears. Double-click the the row corresponding to the script execution job to view the Script Management Job status page. Click the **View Results** link in the **Description** column to view the results of script execution. The Script Execution Job Results page allows you to read and understand the script execution results. From Release 17.2R1 onward, the summary of the job of script execution in Junos Space Platform shows the Total requests, Success, and Script Failure counts. The description of possible status for script execution is as follows:

     - Success—Script successfully executed on devices.
     - Failure—Unable to execute the script on the device because the device is down or not reachable.
     - Script Failure—Script executed on the device, but the execution resulted in an error.

     Click the [X] icon to close this page.

   - Click **OK** to go back to the Scripts page.

You can export details about the execution of a script as a comma-separated values (CSV) file to your local file system:

1. On the Junos Space Platform UI, select **Jobs** > **Job Management**.

   The Job Management page appears.

2. Double-click the row corresponding to the script execution job.

   The Script Management Job Status page appears. The status of the job is Success, Script Failure, or Failure. If there is an error, the View Job Details page displays an error message. For more information about the error messages, see "Common Error Messages in Device-Related Operations" on page 992.

3. Click **Export as CSV**.

   You are prompted to save the file.

4. Click **OK** on the File Save page to save the file to your local file system.

5. After you save the file, to return to the Job Management page, click **OK** on the **Exporting Script Job** page.

   Use an application such as Microsoft Excel to open the file from your local system. Typically, you can view the script output in the Description column of this file.

You can view details of script execution tasks from the Device Management page (Devices > Device Management) by selecting one or more devices and selecting **View Script Executions** from the shortcut menu (Devices > Device Management > Select a device > Device Inventory). This option displays only the results of op scripts executed on the device and not the commit or event scripts.

Release History Table

Release	Description
18.2	From Junos Space Platform Release 18.2R1 onward, you can select devices based on saved filters
17.2	From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.
17.2	From Release 17.2R1 onward, the summary of the job of script execution in Junos Space Platform shows the Total requests, Success, and Script Failure counts.

RELATED DOCUMENTATION

Enabling Scripts on Devices | **696**

Executing Scripts on Devices Locally with JUISE | **704**

Executing Scripts on Devices Locally with JUISE

Junos Space Network Management Platform comes integrated with the Junos OS User Interface Scripting Environment (JUISE)—that is, juise-0.3.10-1 version, which enables you to execute a script on a remote device from the Junos Space server without having to stage the script on the device. To execute a script on a remote device, the following conditions must be met:

- The device should be reachable from the Junos Space server.
- The **@ISLOCAL** annotation marked within the script must be set to true. That is, the script must contain the following text:

  /* @ISLOCAL = "true" */

  When this annotation is set to false, you have to first stage the script on a device and then execute it. For more information about script annotations, see “Script Annotations” on page 721.

  From the Junos Space UI, you can identify the scripts that can be executed locally by looking at the value in the **Execution Type** column on the Scripts page. For scripts that can be executed locally without being staged from the Junos Space server, the value is **Local**.

By default, JUISE is installed when you install or upgrade to Junos Space Release 13.1 or later versions.

> **NOTE:** You can execute only SLAX scripts (*.slax) by using JUISE.

To execute scripts on Junos OS devices with JUISE:

1. On the Junos Space Network Management Platform UI, select **Images and Scripts** > **Scripts**.

   The Scripts page appears, displaying the scripts that you imported into Junos Space Network Management Platform.

2. Select the op script that you want to execute on a device.

   > **TIP:** Identify and select only those scripts that have **Local** displayed in the **Execution Type** column.

3. Select **Execute Script on Devices** from the Actions menu.

   The Execute Script on Device(s) page appears.

4. Select the devices on which you want the script to be executed, by using one of the following selection modes—manually, on the basis of tags, or by using the comma-separated values (CSV) file. These options are mutually exclusive. If you select one, the others are disabled.

   > **NOTE:** By default, the **Select by Device** option is selected and the complete list of devices is displayed.

   - To select devices manually:
     - Click the **Select by Device** option and select the device(s) that have the script staged on them. The Select Devices status bar shows the total number of devices that you selected; the status bar is dynamically updated as you select the devices.
     - To select all the devices, select the check box in the column header next to the Host Name column.
   - To select devices on the basis of tags:
     a. Click the **Select by Tags** option. The Select by tags list is activated.

     b. Click the arrow on the **Select by Tags** list. A list of tags defined on devices in the Junos Space system appears, displaying two categories of tags—Public and Private.

> **NOTE:** If no tags are displayed, then it means that none of the devices is associated with any tag. You need to tag the devices on the Device Management page before you can use the **Select by Tags** option.

c. To select tags, perform one of the following actions :

- Select the check boxes next to the tag names to select the desired tags and click **OK**.
- To search for a specific tag, enter the first few letters of the tag name in the **Select by Tags** field to the left of the **OK** button. If a match is found, a suggestion is made. Select the suggested match and click **OK**.

As you select the tags, the total number of devices associated with the selected tags appears just above the device display table. For example, if there are six devices associated with the selected tags, then **6 items selected** is displayed.

The selected tags appear next to the **Tags Selected** label. An [X] icon appears after each tag name. You can click the [X] icon to clear any tag from the list. The device count decrements accordingly.

The device display table displays the devices associated with the selected tags.

- To select devices by using a CSV file:

a. Select the **Select by CSV** option.

b. Click **Browse** to navigate to the file location on your computer and select the CSV file containing the list of devices on which you want to execute the script.

> **TIP:** For a sample CSV file, click the **Sample CSV** link. You are prompted to save the file. Save the file to your computer and open it by using an application such as Microsoft Excel.

c. Click **Upload** to upload the CSV file.

5. (Optional) To specify values for the parameters for script execution, click **Enter Parameter Value** for each parameter.

6. To schedule a time to execute the script, select the **Schedule at a later time** check box and use the calendar icon and drop-down list respectively to specify the date and time when you want the script to be executed.

7. Click **Execute**.

   The selected scripts are executed on the devices, and the Execute Script Information dialog box displays a link to the job.

   Perform one of the following actions on the Execute Script Information dialog box:

   - To verify the status of the job, click the ***job ID*** link.

     The Job Management page appears. Double-click the the row corresponding to the script execution job to view the Script Management Job status page. Click the **View Results** link in the **Description** column to view the results of script execution. The Script Execution Job Results page allows you to read and understand the script execution results. From Release 17.2R1 onward, the summary of the job of script execution in Junos Space Platform shows the Total requests, Success, and Script Failure counts. The description of possible status for script execution is as follows:

     - Success - Script successfully executed on device(s).
     - Failure – Unable to execute the script on the device because device is down or not reachable
     - Script Failure – Script executed on the device, but the execution resulted in an error.

     Click the [X] icon to close this page.

   - Click **OK** to go back to the Scripts page.

To export details about the execution of a script as a comma-separated values (CSV) file to your computer:

1. On the Junos Space Platform UI, select **Jobs** > **Job Management**.

   The Job Management page appears.

2. Double-click the row corresponding to the script execution job.

   The Script Management Job Status page appears. The status of the job is Success, Script Failure, or Failure.

3. Click **Export as CSV**.

   You are prompted to save the file.

4. Click **OK** in the File Save dialog box to save the file to your computer.

5. After you save the file, to return to the Job Management page, click **OK** in the **Exporting Script Job** dialog box.

Use an application such as Microsoft Excel to open the file from your computer. Typically, you can view the script output in the Description column of this file.

Release History Table

Release	Description
17.2	From Release 17.2R1 onward, the summary of the job of script execution in Junos Space Platform shows the Total requests, Success, and Script Failure counts.

RELATED DOCUMENTATION

Scripts Overview | 673

Executing Scripts on Devices | 700

Viewing Execution Results

You can use Junos Space Network Management Platform to trigger the execution of op scripts on one or more devices simultaneously. You can also view the execution results of the script.

To view the execution results:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Scripts**.

   The **Scripts** page appears.

2. Click the **View Execution Results** icon.

   The **View Execution Results** page appears. This page displays the execution history that includes script version, device name, script name, execution status, job result, execution start time and end time.

   The fields Device Name, Script Name, Category, Version, and Status have the drop down list enabled with the filter option that has an input field where you can enter the filter criteria. If you apply the filters, the table contents display only the values that match the filter criteria. The fields Results, Execution Start Time, and Execution End Time do not support the filter option.

   Table 86 describes the information that appears on the View Execution Results page.

   Table 86: View Execution Results Page Fields

Field	Description
Device Name	Name of the device on which the script is executed

Table 86: View Execution Results Page Fields *(continued)*

Field	Description
Script Name	Name of the script
Category	Category of the script
Version	Executed version of script
Status	Script execution job status
Results	Contains a link to view the script execution results
Execution Start Time	The time at which the execution of the script started
Execution End Time	The time at which the execution of the script ended

3. Click the **View** link in the **Results** column to view the detailed execution results.

   The Script Execution Job Results dialog box appears and displays the results of the script execution. You can read and understand the script execution results. Click the [X] icon to close this dialog box.

You can click **Scripts** on the breadcrumbs at the top of the page to return to the Scripts page.

RELATED DOCUMENTATION

Executing Scripts on Devices | 700
Scripts Overview | 673

Exporting Scripts in .tar Format

You can use Junos Space Network Management Platform to export the contents of multiple scripts and save them on your computer.

To export the contents of scripts in .tar format:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Scripts**.

   The Scripts page appears, displaying the scripts that you imported into Junos Space Platform.

2. Select the scripts that you want to export.

3. Select **Export Scripts** from the Actions menu.

   The **Export Scripts** dialog box prompts you for confirmation.

4. Click **Export**.

   The **File Open** dialog box enables you to save the script files in .tar format and the **Export Scripts Job Status** dialog box displays the status of this task.

   By default, the latest versions of the scripts are exported.

5. Click **OK** in the File Open dialog box to save the file to your computer. Alternatively, you can save the .tar file by clicking the **Download** link in the Export Scripts Job Status dialog box.

6. Perform one of the following actions in the Export Scripts Job Status dialog box:

   - To view the status of the Export Scripts job on the Job Management page, click the progress bar in this dialog box.
   - To return to the Scripts page, click the X icon in this dialog box.

Navigate to the folder on your computer and unzip the files to view the contents of the script.

RELATED DOCUMENTATION

Scripts Overview | 673

Viewing Device Association of Scripts

Junos Space Network Management Platform enables you to view the details of scripts that are saved on the Junos Space server, as well as those that are staged on devices. You can view the script-device association to understand what scripts are staged or enabled on what devices.

To view devices that are associated with scripts:

1. On the Junos Space Network Management Platform UI, select **Images and Scripts** > **Scripts**.

   The Scripts page appears.

2. Select a script.

   NOTE: Make sure that the script is previously staged to the devices using Junos Space Platform.

3. Select **View Associated Devices** from the Actions menu. You can also click **View** in the **Associations** column on the Scripts page to view the associated devices for a single script.

   The View Associated Devices page appears with valid Script - Device(s) association details, which include script name, script type, category, host name, IP address, platform, software version, correct staged script version, latest script version, domain, and activation status.

4. Click **Back** to go back to the **Scripts** page.

RELATED DOCUMENTATION

Scripts Overview | 673
Staging Scripts on Devices | 689

Marking and Unmarking Scripts as Favorite

IN THIS SECTION

Marking Scripts as Favorite | 712
Unmarking Scripts Marked as Favorite | 712

In Junos Space Network Management Platform you can easily identify and group the scripts that you want to stage to devices by marking them as favorite. You can use the My Favorite private tag to mark these

scripts. After tagging the scripts, you can search for and use the tagged scripts in all your tasks that support selection by tags. You can unmark the scripts when you no longer need to identify or group them separately.

This topic describes the following tasks:

Marking Scripts as Favorite

To mark scripts as favorite:

1. On the Junos Space Platform UI, select **Images and Scripts > Scripts**.

   The Scripts page appears, displaying scripts that exist in the Junos Space Platform database.

2. Select the scripts that you want to mark as favorite.

3. Select **Mark as Favorite** from the Actions menu.

   The Mark as Favorite dialog box appears. The name of the tag is set to My Favorite and, by default, the tag is private.

4. (Optional) In the **Description** field, enter a description.

5. Click **Apply Tag**.

   The Mark as Favorite pop-up window appears, displaying a confirmation message that the selected scripts are successfully marked as favorite.

6. Click **OK**.

   The selected scripts are tagged as My Favorite.

   The scripts that you tagged as favorite are displayed in the Tag view on the Scripts page. You can also view the number of objects that are tagged as My Favorite.

Unmarking Scripts Marked as Favorite

To unmark scripts that are marked as favorite:

1. On the Junos Space Platform UI, select **Images and Scripts > Scripts**.

   The Scripts page that appears displays scripts that exist in the Junos Space Platform database.

2. Select the scripts that you want to unmark as favorite.

3. Select **Unmark as Favorite** from the Actions menu.

The Unmark as Favorite pop-up window appears, displaying a confirmation message that the selected scripts are successfully unmarked as favorite.

4. Click **OK**.

   The selected scripts are no longer tagged as My Favorite.

You return to the Scripts page on the Junos Space GUI.

RELATED DOCUMENTATION

Scripts Overview | 673

Importing Scripts to Junos Space | 676

Disabling Scripts on Devices

After you deploy scripts on devices, you can use Junos Space Network Management Platform to disable these scripts on one or more devices simultaneously.

When you disable scripts using Junos Space Platform, the configuration added on the device is similar to the following:
For example, for a file named bgp-active.slax, the configuration added is:
user@host# delete system scripts commit file bgp-active.slax

CAUTION: If the filename of the selected script matches that of any script present on the device, then the script on the device is disabled regardless of its contents.

To disable scripts on devices:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Scripts**.

   The Scripts page appears, displaying the scripts that you imported into Junos Space Platform.

2. Select one or more scripts that you want to disable on devices.
3. Select **Disable Scripts on Devices** from the Actions menu.

   The Disable Scripts on Device(s) page appears. Only those devices that have the selected scripts enabled on them are listed.

   If the selected scripts are already disabled on the devices, then Junos Space displays the following message instead of the Disable Scripts on Device(s) page:

Device(s) having all the selected staged script(s) already have them in disabled state.

4. Select the devices on which you want the script to be disabled, by using one of the following selection modes—manually, on the basis of tags, or by using the comma-separated values (CSV) file. These options are mutually exclusive. If you select one, the others are disabled.

   > **NOTE:** By default, the **Select Device Manually** option is selected and the list of devices that can be selected is displayed.

   - To select devices manually:
     - Click the **Select Device Manually** option and select the devices on which you want to disable the script. The Select Devices status bar shows the total number of devices that you selected; the status bar is dynamically updated as you select the devices.
     - To select all devices, select the check box in the column header next to the Host Name column.
   - To select devices on the basis of tags:
     1. Click the **Select by Tags** option.

        The Select by tags list is activated.

     2. Click the arrow on the **Select by Tags** list. A list of tags defined on devices in the Junos Space system appears, displaying two categories of tags—Public and Private.

        > **NOTE:** If no tags are displayed, then it means that none of the devices is associated with any tag. You need to tag the devices on the Device Management page before you can use the **Select by Tags** option.

     3. To select tags, perform one of the following actions:
        - Select the check boxes next to the tag names to select the desired tags and click **OK**.
        - To search for a specific tag, enter the first few letters of the tag name in the **Select by Tags** field to the left of the **OK** button. If a match is found, a suggestion is made. Select the suggested match and click **OK**.

        As you select the tags, the total number of devices associated with the selected tags appears just above the device display table. For example, if there are six devices associated with the selected tags, then **6 items selected** is displayed.

        The selected tags appear next to the **Tags Selected** label. An [X] icon appears after each tag name. You can click the [X] icon to clear any tag from the list. The device count decrements accordingly.

The device display table displays the devices associated with the selected tags.

- To select devices by using a CSV file:

  1. Select the **Select by CSV** option.

  2. Click **Browse** to navigate to the file location on your computer and select the CSV file containing the list of devices on which you want to disable the script.

     TIP: For a sample CSV file, click the **Sample CSV** link. You are prompted to save the file. Save the file to your computer and open it by using an application such as Microsoft Excel.

  3. Click **Upload** to upload the CSV file.

     From Release 16.1R2 onward, when you upload a CSV file to select devices from, Junos Space Platform verifies the devices in the CSV file. If the CSV file contains devices to which the changes do not apply, a warning message appears which says "Few devices are not selected due to precondition failure. Please click "View inapplicable devices" for more details." You can click the **View inapplicable devices** link to review the list of devices that are excluded from the update.

5. (Optional) To schedule a time for disabling the script, select the **Schedule at a later time** check box and use the calendar icon and drop-down list respectively to specify the date and time when you want the script to be disabled.
6. Click **Disable**. The **Disable** button is unavailable if you have not selected any devices. Select the devices on which you want to disable the scripts before you click **Disable**.

   The selected scripts are disabled on the devices, and the Disable Scripts Information dialog box displays a link to the job ID.
7. Perform one of the following actions on the Disable Scripts Information dialog box:

   - To verify the status of this job, click the ***job ID*** on this dialog box.

     The Job Management page appears. Double-click the job pertaining to the disabling operation. The Script Management Job Status page appears and the **Description** column on this page displays whether or not the script is disabled successfully and reasons for failure (if disabling of the script had failed). If there is an error, the View Job Details page displays an error message. For more information about the error messages, see “Common Error Messages in Device-Related Operations” on page 992.

   - Click **OK** to go back to the Scripts page.

RELATED DOCUMENTATION

Scripts Overview | 673

Removing Scripts from Devices

You can use Junos Space Network Management Platform to remove scripts from devices on which they are staged or enabled.

CAUTION: If the filename of the selected script matches that of any script present on the device, then the script on the device is removed regardless of its contents.

To remove scripts from devices:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Scripts**.

   The Scripts page appears, displaying the scripts that you imported into Junos Space Platform.
2. Select the script or scripts that you want to remove.
3. Right-click your selection or use the Actions menu, and select **Remove Scripts from Devices**.

   The Remove Scripts from Device(s) page appears and lists the devices the script is associated with.

   NOTE: If you select multiple scripts for removal, only those devices that are associated with all the scripts are listed in the Remove Scripts from Device(s) page. If a device is not associated with even one of the selected scripts, it is not listed.

4. Select the devices from which you want the script to be removed, by using one of the following selection modes—manually, on the basis of tags, or by using the comma-separated values (CSV) file. These options are mutually exclusive. If you select one, the others are disabled.

   NOTE: By default, the **Select Device Manually** option is selected and the list of devices that can be selected is displayed. For multiple selection, only commonly associated devices are listed.

   - To select devices manually:

- Click the **Select Device Manually** option and select the device(s) that have the script staged on them. The Select Devices status bar shows the total number of devices that you selected; the status bar is dynamically updated as you select the devices.
- To select all the devices, select the check box in the column header next to the Host Name column.

- To select devices on the basis of tags:

  1. Click the **Select by Tags** option.

     The Select by tags list is activated.

  2. Click the arrow on the **Select by Tags** list. A list of tags defined on devices in the Junos Space system appears, displaying two categories of tags—Public and Private.

     > **NOTE:** No tag is displayed if none of the devices is associated with any tag. You need to tag the devices on the Device Management page before you can use the **Select by Tags** option.

  3. To select tags, perform one of the following actions :
     - Select the check boxes next to the names of tags that you want to select and and click **OK**.
     - To search for a specific tag, enter the first few letters of the tag name in the **Select by Tags** field to the left of the **OK** button. If a match is found, a suggestion is made. Select the suggested match and click **OK**.

     As you select the tags, the total number of devices associated with the selected tags appears just above the device display table. For example, if there are six devices associated with the selected tags, then **6 items selected** is displayed.

     The selected tags appear next to the **Tags Selected** label. An [X] icon appears after each tag name. You can click the [X] icon to clear any tag from the list. The device count is updated accordingly.

     The device display table displays the devices associated with the selected tags.

- From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.

  To select devices by using a CSV file:

  1. Select the **Select by CSV** option.

  2. Click **Browse** to navigate to the file location on your computer and select the CSV file containing the list of devices from which you want to remove the script.

> **TIP:** For a sample CSV file, click the **Sample CSV** link. You are prompted to save the file. Save the file to your computer and open it by using an application such as Microsoft Excel.

3. Click **Upload** to upload the CSV file.

   From Release 16.1R2 onward, when you upload a CSV file to select devices from, Junos Space Platform verifies the devices in the CSV file. If the CSV file contains devices to which the changes do not apply, a warning message appears which says **Few devices are not selected due to precondition failure. Please click "View inapplicable devices" for more details.**

   You can click the **View inapplicable devices** link to review the list of devices that are excluded from the update. The reason for exclusion is listed as an error message against each device.

- From Junos Space Platform Release 18.2R1 onward, you can select devices based on saved filters

  To select devices by using a saved filter:

  1. Select the **Select by Filter** option.

  2. Select the filter from the list of saved filters.

     The devices associated with the selected filter appears in the grid.

5. Select the **Force Remove** check box to remove the script-device association from Junos Space Platform even if it is unable to remove the scripts from the devices due to connectivity issues. You need to turn this option on before you remove the scripts. The script-device association is removed regardless of whether this operation fails or not.
6. Click **Remove**.

   The script is removed from the selected devices, and the Remove Scripts Information page appears, which displays a job ID link.

   Perform one of the following actions on the Remove Scripts Information page:

   - Click the ***job ID*** link to view the status of the script removal operation on the Job Management page.

     The Job Management page appears. Double-click the row corresponding to the job pertaining to the removal operation. The Script Management Job Status page appears and the **Description** column on this page displays whether or not the script is removed successfully and reasons for failure (if the removal of the script failed).

   - Click **OK** to return to the Scripts page.

From the Junos Space Platform UI, you can verify the device association details of the scripts removed from the devices. On the **Scripts** page, click **View** in the **Associations** column of the removed script. The **View Associated Devices** page is displayed, where you can verify that the device associations are removed.

If the script removal task fails, you can identify the reason for failure by viewing the job details from the Job Management page. If there is an error, the View Job Details page displays an error message. For more information about the error messages, see "Common Error Messages in Device-Related Operations" on page 992.

For more information about viewing job details, see "Viewing Jobs" on page 972 .

On the Job Management page, you can export details about the removal of a script as a comma-separated values (CSV) file to your local file system:

1. On the Junos Space Platform UI, select **Jobs** > **Job Management**.

   The Job Management page appears.

2. Double-click the row corresponding to the script removal job.

   The Script Management Job Status page appears.

3. Click **Export as CSV**.

   You are prompted to save the file.

4. Click **OK** on the File Save page to save the file to your computer.

5. After you save the file, to return to the Job Management page, click **OK** on the **Exporting Script Job** page.

   Use an application such as Microsoft Excel to open the downloaded file from your computer.

Release History Table

Release	Description
18.2	From Junos Space Platform Release 18.2R1 onward, you can select devices based on saved filters
17.2	From Junos Space Platform Release 17.2R1 onward, when you select devices by CSV, you can choose to select all managed devices. Select the **Include All Managed Devices** check box to list all managed devices for selection.

RELATED DOCUMENTATION

Staging Scripts on Devices | 689
Scripts Overview | 673

Deleting Scripts

You can use Junos Space Network Management Platform to delete the scripts that you import into the Junos Space server. When you delete a script, all versions of that script and the checksum verification results associated with that script are deleted.

To delete scripts from the Junos Space server:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Scripts**.

   The Scripts page appears, displaying the scripts that you imported into Junos Space Platform.

2. Select the scripts that you want to delete.

   > **NOTE:** Only the scripts that are not associated with any of the devices can be deleted. You must remove scripts from the device before deleting the scripts from Junos Space Platform. When you delete a script, all versions of that script and the checksum verification results associated with that script are deleted.

3. Click the **Delete Scripts** icon.

   If you have not removed scripts from the device before deleting the scripts from Junos Space Platform, you receive an action failure message.

   The **Delete Device Scripts** dialog box appears, listing the scripts that you chose for deletion.

4. Click **Confirm** on the Delete Device Scripts dialog box.

   The selected scripts are deleted and the **Jobs** dialog box displays a job ID link. You can click the link to view the status of the delete operation on the Job Management page.

   If the deletion of the script fails, you can identify the reason for failure by double-clicking the row containing the job on the Job Management page. The Job Details page appears and displays the reason for failure in the **Description** column. However, if the script is deleted successfully, then the Job Details page displays the following information in this column:
   Script deleted successfully
   The Job Details page supports sorting of data in all columns in ascending or descending order.

You can select **Images and Scripts** > **Scripts** on the left pane of the Junos Space GUI to return to the Scripts page.

RELATED DOCUMENTATION

Modifying Scripts | 684

Script Annotations

IN THIS SECTION

- Script Execution Types | 724
- Variable Context | 725
- Local Script Execution | 726
- Nesting Variables | 727

Script annotations are used to specify the metadata of a script. They are embedded in scripts. They are parsed and stored in the Junos Space Network Management Platform database while scripts are modified or imported. An annotation uses the following syntax:

/* @[ANNOTATION]= "<ANNOTATION CONTENT>" */

An annotation can be provided anywhere in the script.

Annotations are used to specify the name, description, and confirmation text of a script and the context in which the script can be applied. For an example script with an annotation, see "Script Example" on page 727. Table 87 displays the types of script annotations with their descriptions.

Table 87: Types of Script Annotations

Annotation	Description
@CONTEXT	This annotation is used to specify the context in which the script can be applied. When the context is not specified, the default context is taken as /device. Example: `/* @CONTEXT = "/device/chassis-inventory/chassis/chassis-module[starts-with (name,"FPC")]/chassis-sub-module[starts-with(name,"PIC")]" */` **NOTE:** You can execute scripts on more than 200 devices only if the script context is /, //, or /device and no device-specific or entity-specific parameters are specified.

Table 87: Types of Script Annotations *(continued)*

Annotation	Description
@NAME	This annotation is used to specify the descriptive name of the script. Example: **/* @NAME = "Put PIC Offline" */**
@CATEGORY	This annotation is used to specify the category to which the script belongs. This annotation enables you to group scripts based on any criteria. The annotation cannot exceed 255 characters. It can contain only letters and numbers and can include hyphen (-), underscore (_), space ( ), or period (.). Example: **/* @CATEGORY = "Interface Configuration" */**
@DESCRIPTION	This annotation is used to specify a description of the script. Example: **/* @DESCRIPTION = "Take PIC offline." */**
@CONFIRMATION	This annotation is used to specify the confirmation text of the script. That is, the text that must be displayed when an attempt is made to execute the script. When this field is not provided, no confirmation text is shown when the script is executed. This can be used to create warnings for certain scripts. Example: **/* @CONFIRMATION = "Are you sure that you want to take the PIC offline?" */**
@EXECUTIONTYPE	This annotation is used to specify the type of execution. The types of execution are GROUPEDEXECUTION and SINGLEEXECUTION. When this annotation is not specified, the default option is SINGLEEXECUTION. Example: **/* @EXECUTIONTYPE = "SINGLEEXECUTION" */**

Table 87: Types of Script Annotations *(continued)*

Annotation	Description
@GROUPBYDEVICE	This annotation is used to specify whether the script must be executed simultaneously or sequentially on the selected devices. The annotation works only for scripts for which the execution type is GROUPEDEXECUTION and @ISLOCAL is true. You can add the GROUPBYDEVICE annotation from Junos Space Network Management Platform Release 15.2R1 onward. If the annotation is set to TRUE, the script is executed on the selected devices at the same time. If set to FALSE or if the annotation is not included in the script, the script is executed sequentially on the selected devices. Example: **/* @EXECUTIONTYPE = "GROUPEDEXECUTION" */** **/* @GROUPBYDEVICE="TRUE" */** **/* @ISLOCAL = "true" */**
@ISLOCAL	This annotation is used to define whether the script is to be executed locally or staged on the device. This could be True or False. Example: **/*@ISLOCAL="true"*/**
@VARIABLECONTEXT	This annotation is used to define the context of a variable. Example: `/*@VARIABLECONTEXT="[{'name':'XPATHVARIABLE1','defaultvalue':'mydefaultvalue','parameterscope':'devicespecific'},{'name':'XPATHVARIABLE2','configuredvaluexpath':'/device/interface-information/physical-interface/name/text()','parameterscope':'entityspecific'},{'name':'XPATHVARIABLE3','selectionvaluesxpath':'/device/interface-information/physical-interface/name/text()','parameterscope':'global'}]"*/`
@PASSSPACEAUTHHEADER	This annotation is specific to local scripts. If the annotation is set to True, then the $JSESSIONSSO and $JSESSIONID script variables are set. Example: **/*@PASSSPACEAUTHHEADER="true"*/** This annotation also provides the virtual IP address of the cluster in $VIP.
@PASSDEVICECREDENTIALS	This annotation is specific to local scripts. If the annotation is set to true, Junos Space Platform sets the device credentials to *$credentials* and *$deviceipmap* variable (that is, $deviceipmap= '{"192.168.0.210":"Device1",...}').. Example: **/*@ PASSDEVICECREDENTIALS ="true"*/**

Table 87: Types of Script Annotations *(continued)*

Annotation	Description
@PROMOTE	This annotation is used to define whether the script is available for execution as a right-click action. This only works for scripts with the @EXECUTIONTYPE = "SINGLEEXECUTION" annotation.
@ONCLOSESTRING	This annotation is used when the user wants the script execution result page to be closed automatically after the expected result is received. The @ONCLOSESTRING annotation contains a string. This string is compared with the script execution results. When the specified string appears in the script output, the script execution result page is automatically closed. The @ONCLOSESTRING annotation is useful for script promotion. For example, if a user has included the @ONCLOSESTRING annotation in the Reboot script containing a string that is displayed on successful execution of the script and executes the promoted Reboot script. The script execution result page closes by itself automatically and the reboot command is sent to the device successfully. If the script is not executed successfully, the reason for failure is displayed in the script execution result window. This further improves user experience by reducing the number of clicks required by the user to complete an action.
@FAILJOBSTRING	This annotation is used to specify an arbitrary string which if present in the script output identifies the script execution as failure. The @FAILJOBSRTING annotation can take an arbitrary string value that does not exceed 255 characters. Because the string comparison is case sensitive, ensure that the string specified for @FAILJOBSTRING and the one in the script output use the same casing. The value of the @FAILJOBSRTING annotation can also be used as a tag name. If the script output contains the tag, the corresponding job is marked as failure. **/* @FAILJOBSTRING = "Reason for Job Failure" */** **/* @FAILJOBSTRING = "Failed while creating vlan" */**

Script Execution Types

With the SINGLEEXECUTION script execution type, the script can be executed only on a single element at a time. This is helpful if the script developer wants to ensure that the script execution is not executed for multiple elements simultaneously.

With the GROUPEDEXECUTION script execution type, the script is executed for a group of devices simultaneously. The context of the elements belonging to the group is passed as an expression to the

$CONTEXT variable in the script. This way, the script is provided with the elements for which the script should be executed.

For example, for GROUPEDEXECUTION, the context structure could be as follows:

```
/device[name="EX4200-20"]/interface-information/physical-interface[name="ge-0/0/11"]|
/device[name="EX4200-20"]/interface-information/physical-interface[name="ge-0/0/12"],
/device[name="EX4200-240"]/interface-information/physical-interface[name="ge-0/0/5"]|
/device[name="EX4200-240"]/interface-information/physical-interface[name="ge-0/0/6"].
```

Variable Context

The variable context defines what input the script is expecting from the user. This context can be used to autopopulate user-input options. This behavior is similar to that of the parameters in CLI Configlets. The variable context is defined using the @VARIABLECONTEXT annotation. The options are given in the following format:

@VARIABLECONTEXT = "[{'name':'<variable-name-1>',
'<option-1-1>':'<value-1-1>','<option-1-2>':'<value-1-2>',....,},.....,{'name':'<variable-name-n>',
'<option-n-1>':'<value-n-1>','<option-n-2>':'<value-n-2>',....,}]"

Table 88 explains the possible options.

Table 88: Variable Context Options

Option	Description
configuredvaluexpath	This specifies the XPath (with reference to the device XML) from which the value of the parameter must be fetched.
defaultvalue	The behavior is the same as that of configured value of XPath except that the value is given explicitly. This is considered only when "configuredvaluexpath" is not specified.
selectionvaluesxpath	This contains the XPath (with reference to the device XML) to fetch the set of values for populating the options.
selectionvalues	This is the same as the "selectionvalues" except that the comma-separated values are given explicitly.
parameterscope	This is used to specify the scope of a parameter. • entityspecific – A value is required for each individual entity. • devicespecific – A value is required for each individual device. • global – Only a single value is required for all entities.

Table 88: Variable Context Options *(continued)*

Option	Description
password	Use this option to allow the user to enter a password before executing the scripts. This obscures or displays the input parameters that you enter when you execute an op script. If you configure an op script with the @VARIABLECONTEXT script annotation for an input parameter with the "password" option, the input parameters that you enter in this field are obscured or displayed depending on the following values: • no – The input parameter entered is not obscured. • yes – The input parameter entered in this field is obscured. The configuredvaluexpath, defaultvalue, selectionvaluesxpath, and selectionvalues options are ignored. • Confirm – You need to enter the same input parameter twice. The input parameter entered is obscured. The configuredvaluexpath, defaultvalue, selectionvaluesxpath, and selectionvalues options are ignored.

Local Script Execution

With Junos Space, you can execute op scripts in one or more devices simultaneously without staging and enabling the scripts. To do this, you use the local script execution feature. This feature enables you to execute the script locally in the Junos Space server. The @ISLOCAL annotation in the script must be set to true to differentiate normal script from the local script:

/*@ISLOCAL="true"*/

Local scripts run directly in the Junos Space server, so you do not need to stage, enable, or disable these scripts. If a script that is already staged is modified using the @ISLOCAL annotation, the update is rejected.

You can execute local scripts on one or more selected devices. For a cluster setup, you need to execute the scripts on a VIP node.

For the GROUPEDEXECUTION execution type, the device IP address list is passed as a parameter. The script opens an internal connection before interacting with the device.

You can execute local scripts with the GROUPEDEXECUTION execution type on multiple devices simultaneously by setting GROUPBYDEVICE to TRUE. If the GROUPBYDEVICE annotation is set to FALSE or if the annotation does not appear in the script, the script is executed sequentially on the selected devices.

NOTE: Local scripts can be executed on devices with Junos Space–initiated connection.

Nesting Variables

You can use the XPath context to define the default option or the selectable options of a variable that are displayed on the script execution page. This XPath could have dependencies on other variables. Consider the following example:

A script requires two inputs: Physical Interface (Input-1) and a Logical Interface (Input-2) that is part of the selected Physical Interface (Input-1). You first define a variable *PHYINT* to get the name of the physical interface and a variable *LOGINT* to get the name of the logical interface. You then define the SELECTIONVALUESXPATH for PHYINT as **/device/interface-information/physical-interface/name/text()**. Select a value from the options listed by the XPath. Because the selection values listed for the *LOGINT* variable is dependent on the value selected for *PHYINT*, you define the SELECTIONVALUESXPATH of LOGINT as **/device/configuration/interfaces/interface[name='$PHYINT']/unit/name/text()**. This ensures that only the logical interfaces of the selected physical interface are listed.

> **NOTE:** When using the $INTERFACE, $UNIT, Configured Value XPath, Invisible Params, and Selection fields, the variable definition in the CLI Configlet Editor should contain **.get(0)** to fetch the value from the array. For example, **$INTERFACE.get(0)**.

Release History Table

Release	Description
15.2R1	You can add the GROUPBYDEVICE annotation from Junos Space Network Management Platform Release 15.2R1 onward.

RELATED DOCUMENTATION

Script Example | 727
Scripts Overview | 673

Script Example

The following is the script to take PIC offline.

A script has four associated attributes, @CONTEXT, @NAME, @DESCRIPTION and @CONFIRMATION. These attributes are given within comments (/* */).

The @CONTEXT attribute states, what context the script can be executed on.

The @NAME attribute defines the descriptive name of the script and @DESCRIPTION defines the description of the script.

The @CONFIRMATION defines the text that should be shown to the user for confirmation before the script gets executed. This is to prevent accidental execution of scripts.

```
Version 1.0;
import "../import/junos.xsl";
import "cim-lib.slax";

/* Junos Space specific context, name and description */
/* @CONTEXT = "/device/chassis-inventory/chassis/chassis-module
[starts-with(name,"FPC")]/chassis-sub-module[starts-with(name,"PIC")]" */
/* @NAME = "Put PIC Offline" */
/* @DESCRIPTION = "Take PIC offline." */
/* @CONFIRMATION = "Are you sure that you want to take the PIC offline?" */
/* @EXECUTIONTYPE = "SINGLEEXECUTION" */
/*@VARIABLECONTEXT="[{'name':'XPATHVARIABLE1','defaultvalue':'mydefaultvalue',
'parameterscope':'devicespecific'},
{'name':'XPATHVARIABLE2','configuredvaluexpath':'/device/interface-information/
physical-interface/name/text()','parameterscope':'entityspecific'},
{'name':'XPATHVARIABLE3','selectionvaluesxpath':'/device/interface-information/
physical-interface/name/text()','parameterscope':'global'}]"*/
/* Global variables */
var $scriptname = "op-pic-offline.slax";
var $results;
var $regex;
var $result-regex;
  var $arguments = {
    <argument> {
      <name> "CONTEXT";
      <description> "The context associated with this script.";
    }
  }
param $CONTEXT;
  match / {
    <op-script-results> {
      var $regex = "/device/chassis-inventory/chassis\\[name=\"(.*)\"\\]/chassis-module\\[name=\"(.*
        ([0-9]+))\"\\]/chassis-sub-module\\[name=\"(.* ([0-9]+))\"\\]";
      var $result-regex = jcs:regex( $regex , $CONTEXT );
      /* Request PIC offline */
      var $command = {
        <command> "request chassis pic offline fpc-slot " _ $result-regex[4] _ " pic-slot " _ $result-regex[6];
```

```
        }
        var $results = jcs:invoke($command);
        /* Error check */
        call cim:error-check( $results-to-check = $results , $sev = "external.error" , $script = $scriptname , $cmd =
          $command , $log = "no" );
        <output> {
          <HTML> {
            <HEAD> {
              <title> "PIC offline";
              <style type="text/css"> {
                expr "body { font-family: Verdana, Georgia, Arial, sans-serif;font-size: 12px;color:#fff;}";
                expr "td { font-family: Verdana, Georgia, Arial, sans-serif;font-size: 12px;color:#fff;}";
                expr "p { font-family: Verdana, Georgia, Arial, sans-serif;font-size: 12px;color:#fff;}";
              }
            }
            <BODY bgcolor="transparent"> {
              <p> {
                copy-of $results;
              }
            }
          }
        }
      }
    }
```

RELATED DOCUMENTATION

Script Annotations | 721

Scripts Overview | 673

CHAPTER 38

Managing Operations

IN THIS CHAPTER

- Operations Overview | 730
- Creating an Operation | 731
- Importing an Operation | 736
- Viewing an Operation | 738
- Modifying an Operation | 740
- Running an Operation | 740
- Viewing Operation Results | 744
- Copying an Operation | 745
- Exporting an Operation in .tar Format | 746
- Deleting an Operation | 748

Operations Overview

In Junos Space Network Management Platform, a device image is a software installation package that enables you to upgrade to or downgrade from one Junos operating system (Junos OS) release to another. Scripts are configuration and diagnostic automation tools provided by Junos OS.

Junos Space Network Management Platform enables you to perform tasks related to scripts and device images simultaneously, by allowing you to group tasks, such as staging device images and staging or executing scripts, into a single operation. This facilitates efficient use and reuse of tasks that are frequently performed.

Based on the roles assigned to your username, Junos Space Network Management Platform enables or disables different tasks. For more information about the roles that you need to be able to perform any tasks on operations, see “Device Images and Scripts Overview” on page 609.

You can perform the following tasks from the Operations page:

- Create an operation.
- Modify an operation.

- Delete operations.
- Create a copy of an existing operation.
- Execute (or run) an operation.
- Export operations.
- Import an operation.
- Assign an operation to a domain.
- View information about operations in four stages of execution (successful, failed, in progress, and scheduled).
- Tag and untag operations, view operations that are tagged, and delete private tags.

RELATED DOCUMENTATION

Creating an Operation | 731

Modifying an Operation | 740

Running an Operation | 740

Copying an Operation | 745

Viewing Operation Results | 744

Deleting an Operation | 748

Exporting an Operation in .tar Format | 746

Importing an Operation | 736

Scripts Overview | 673

Device Images Overview | 613

Script Bundles Overview | 749

Creating an Operation

Junos Space Network Management Platform enables you to create operations that combine multiple scripts and image tasks, such as deploying images and staging or executing scripts, into a single operation for efficient use and reuse. An operation can also contain other existing operations, as well as tasks for Junos Continuity software packages (JAM packages).

NOTE: An operation can contain any number of scripts and operations, but only one device image.

To create an operation:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Operations**.

   The Operations page appears.

2. Click the **Create Operation** icon.

   The Create Operation dialog box appears.

3. In the **Name** text box, type a name for the operation.

   The operation name cannot exceed 32 characters. The name can contain only letters and numbers and can include a hyphen (-), underscore (_), or period (.). The name cannot start with a space.

4. In the **Description** text box, type a description for the operation.

   The operation description cannot exceed 256 characters. The description can contain only letters and numbers and can include a hyphen (-), underscore (_), period (.), or comma (,).

5. Select the **Mark as important** check box to mark this operation as important.

6. Click the **Add** icon, and select **Script**, **Image**, or **Operation** from the list.

   The Select Scripts, Select Images, or Select Operations dialog box appears depending on what you selected and displays all the Junos Space Platform scripts, images, and operations, respectively, that you can include in the operation.

   - To add a script, click the **Add** icon, and select **Script** from the list.

     The Select Scripts page appears. This page displays all the available scripts on the Junos Space Platform. To search for a specific script, you can enter the search criteria in the Search field on the top right of this page. To clear the search results, click the **x** icon next to the search criteria.

     To select the scripts:

     a. Select the scripts and click **Add** to add your selections to the list.

        You are returned to the Create Operation dialog box.

     b. Click the **Edit** icon next to the script to specify:

- The action that should be performed. The action can be **Stage** (default), **Execute**, or **Remove**.

  > **NOTE:** The **Remove** action is supported only from Junos Space Network Management Platform Release 15.2R1 onward.

- The version of the script to be associated with the operation. If you have opted to stage or execute the script, you can select the version of the script to be staged or executed. By default, the latest version is selected. To change the version, select the required version of the script from the **Version** list. If you are executing the script as part of the operation, select the version that you have staged; else, Junos Space Platform displays an error message when you run the operation.
- Whether the script must be enabled or not. If you have opted to stage or execute the script, you can choose to keep the script enabled on the device or devices. Keep the **Enable Script** check box selected if you want the scripts to be enabled and ready to be executed when you stage them from Junos Space Platform. Clear this check box if you want the scripts to be disabled on the devices. However, before you run the operation, make sure that the scripts are enabled; else, Junos Space Platform displays an error message.
- The Script Return Code. If you have opted to execute the script, then you can configure the script return code, which indicates whether the script execution was a success or failure. Junos Space Platform, by default, returns “Success” when it is able to execute a script successfully. However, you may want to consider the script execution to be a success or a failure only if a specific pattern string is present in the script execution results. You can specify this pattern string in the **Set value** field. This field supports up to a maximum of 255 characters.

  For example, consider you are running a script to verify whether all the interfaces on a device are up. Though the script might execute successfully, you may want to show this script execution as a failure if an interface is down. To achieve this, you can search for the string “down” in the script execution results using the following steps:

  In the **Set Return Code** section:

  a. Select **Failure**.

  b. In the **Set value** field, type **down**.

- Whether the script-device association must be forcibly removed or not. If you have opted to remove the script, you can select the **Force Remove** check box to make sure that the script-device association is removed from Junos Space Platform, irrespective of whether the script is removed successfully or not.

  When you select the Remove option and the script is staged and enabled on the device, Junos Space Platform disables the script on the device, removes the script from the device, and then removes the script-device association. If the script is staged on the device and not enabled,

Junos Space Platform removes the script from the device and then removes the script-device association.

If Junos Space Platform encounters a problem, such as loss of device connectivity, when the script is being disabled or removed, the script-device association might not be removed. To ensure that the script-device association is removed, you must select the Force Remove check box.

c. Click **Save** to save the configuration changes to the script.

- To add a device image or a Junos Continuity software package, click the **Add** icon, and select **Image** from the list. The Select Device Image page appears. This page displays all the images available in Junos Space Platform. To search for a specific image, you can enter the search criteria in the Search field on the top right of this page. To clear the search results, click the **x** icon next to the search criteria.

  NOTE: You can select Junos Continuity software packages by following the procedure for selecting device images.

  To select the device images:

  a. Select the images and click **Add** to add your selections to the list.

  You are returned to the Create Operation dialog box.

  b. Click the **Edit** icon next to the image to specify the action that must be performed. The action can be **Stage**, **Deploy**, or **Undeploy**.

  NOTE:
  - The Undeploy option appears only if you have selected a Junos Continuity software package to be added. The Undeploy option does not appear in the case of other device images.
  - The deployment options that are displayed for Junos Continuity software packages and for device images are different. For more information about specifying deployment options, see “Deploying Device Images” on page 637.

- To add an operation, click the **Add** icon, and select **Operation** from the list. The Select Operations page appears. This page displays all the available operations on the Junos Space Network Management Platform. To search for a specific operation, you can enter the search criteria in the Search field on the top right of this page. To clear the search results, click the **X** icon next to the search criteria.

To select the operations:

a. Select the operations on the **Select Operations** page.

b. Click **Add** to add your selections to the list.

You are returned to the Create Operation dialog box.

> **NOTE:** You cannot edit the child operation from the Create Operation dialog box.

7. You can modify the list of selected scripts, images, and operations by using the icons described in Table 89.

Table 89: Create Operation Dialog Box Icon Descriptions

Icon	Description
	Add scripts, image, and operations to the list.
	Delete the selected script, image, or operation from the list.
	Move the selected script, image, or operation to the row above.
	Move the selected script, image, or operation to the row below.
	Make a copy of the selected script, image, or operation, and include it in the operation.
	Edit the options for deploying or executing the scripts or images in the operation. For scripts, you can edit the action type, script parameters, and their values (success or failure). For images, you can edit the action type and the image staging and deployment options. See "Deploying Device Images" on page 637 for more information. **NOTE:** You cannot edit a child operation.

8. Click **Create** to create the operation.

You are returned to the Operations page. If the operation is successfully created, then you can view the newly added operation on this page. An operation that is marked important appears with a star next to it indicating that this operation takes priority over others (the star appears in the Priority column on the Operations page).

You can verify whether the operation is created with your specifications by double-clicking the operation and viewing its details.

Release History Table

Release	Description
15.2R1	The **Remove** action is supported only from Junos Space Network Management Platform Release 15.2R1 onward.

RELATED DOCUMENTATION

- Operations Overview | **730**
- Modifying an Operation | **740**
- Running an Operation | **740**
- Copying an Operation | **745**
- Viewing Operation Results | **744**
- Deleting an Operation | **748**
- Exporting an Operation in .tar Format | **746**
- Importing an Operation | **736**

Importing an Operation

You can use Junos Space Network Management Platform to import operations to the Junos Space Platform database from your local file system. The operation that you import must be an XML file (for example, operation-test.xml). Before you import operations, make sure that:

- The files are in .xml format
- The objects that are referenced in the operation exist in the Junos Space Platform instance to which you are importing. Else, Junos Space Platform displays an error message and the operation is not imported.

To view the syntax of an operation XML file, you can create and export an operation from Junos Space Platform to your local file system and open the .xml file in an XML editor. For more information about creating and exporting an operation, see "Creating an Operation" on page 731 and "Exporting an Operation in .tar Format" on page 746.

NOTE: If you want to import multiple operations at a time, use the Mozilla Firefox or Google Chrome Web browser. Currently, Internet Explorer does not support selection of multiple files. In addition, note that two operations with the same name cannot be imported into the Junos Space server.

To import operations to Junos Space Platform:

1. On the Junos Space Platform UI, select **Images and Scripts > Operations**.

   The Operations page appears.

2. Click the **Import Operation** icon.

   The Import Operations page appears.

3. Click the **Add Operations** (**+**) icon.

   The Add Operations page appears.

4. Click **Browse** and select the operation file from your local file system.

   NOTE: Use Mozilla Firefox or Google Chrome to import multiple operations. Currently, using Internet Explorer, you can import only a single file at a time.

5. Click **Add Operations**.

   If the selected operation is valid, it is displayed on the Import Operations page. If the selected operation is not valid, you receive a failure notice.

6. Click **Import Operation**.

   If the operation of the same name exists in Junos Space Platform, you are asked whether you want to overwrite the existing operation. Click **Yes** to overwrite; else, click **No**.

7. If the operations are imported successfully, Junos Space Platform displays a success message. Click **OK** on this message.

   However, if the imported operation references an object (script, image, or operation) that is not present in the target Junos Space Platform instance, Junos Space Platform displays an error message and the operation is not imported.

   Sample error message:

No operation file(s) are imported. Referenced operation test-operation-1 in Operation test-operation-nested does not exist!

RELATED DOCUMENTATION

- Operations Overview | 730
- Creating an Operation | 731
- Modifying an Operation | 740
- Running an Operation | 740
- Copying an Operation | 745
- Viewing Operation Results | 744
- Deleting an Operation | 748
- Exporting an Operation in .tar Format | 746

Viewing an Operation

Junos Space Network Management Platform enables you to perform scripts and device images related tasks simultaneously, by allowing you to group tasks, such as staging device images and staging or executing scripts, into a single operation. The Operations page of the Images and Scripts workspace enables you to view and manage these operations in Junos Space Platform.

You can view information about all the operations in Junos Space Platform from the Operations page. To view detailed information about a particular operation, you can use the View Operation Details option.

To view operations from the Operations page:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Operations**.

   The Operations page appears, displaying the operations created in or imported to Junos Space Platform.

   Table 90 describes the fields displayed on the Operations page.

   You can use the filter option on the drop-down lists of all fields except the Priority field, to specify the filter criteria. When you apply the filters, the page displays only the operations that match the filter criteria.

2. Select an operation and click the **View Operation Details** icon, or double-click the operation whose details you want to view.

   The View Operations dialog box appears.

Table 90 also contains the description of fields in the View Operations dialog box.

3. (Optional) Click the arrow next to the script, image, or operation name to view details for the script, image, or operation respectively.

Table 90: Description of Fields on the Operations Page and the View Operations dialog box

Field	Description	Displayed In
Priority	Displays a star icon if the operation is marked as important	**Operations** page
Operation Name	Name of the operation	**Operations** page
Domain	Domain to which the operation is assigned	**Operations** page
Description	Description of the operation	**Operations** page **View Operations** dialog box
Creation Time	Date and time when the operation was created or imported	**Operations** page
Last Updated Time	Date and time when the operation was last modified	**Operations** page
Name	Name of the Operation	**View Operations** dialog box
Mark as important	Values are True or False	**View Operations** dialog box
• **Name** • **Type** • **Action** • **Description**	• Name of the device image or script • Image or Script • Action to be performed on the device image or script • Description of the device image or script	**View Operations** dialog box

RELATED DOCUMENTATION

Operations Overview | 730

Creating an Operation | 731

Modifying an Operation

With Junos Space Network Management Platform you can modify an existing operation by editing the parameters of the operation.

To modify an operation:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Operations**.

   The Operations page displays all the operations in the Junos Space Platform database.

2. Select the operation that you want to modify.

3. Click the **Modify Operation** icon.

4. Modify the necessary parameters. See "Creating an Operation" on page 731 for more information.

5. Click **Modify** to save your changes and return to the Operations page.

   To verify whether your changes are saved, double-click the operation and view the details.

RELATED DOCUMENTATION

- Operations Overview | 730
- Creating an Operation | 731
- Running an Operation | 740
- Copying an Operation | 745
- Viewing Operation Results | 744
- Deleting an Operation | 748
- Exporting an Operation in .tar Format | 746
- Importing an Operation | 736

Running an Operation

Junos Space Network Management Platform allows you to execute (or run) operations existing in the Junos Space Platform database.

To run an operation:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Operations**.

   The Operations page displays all the operations in the Junos Space Platform database.

2. Select the operation that you want to execute.

3. Select **Run Operation** from the Actions menu.

   The Run Operation page appears.

4. Select the device or devices on which you want to execute the operation by using one of the following methods—manually, on the basis of tags, or by using a comma-separated values (CSV) file. These options are mutually exclusive. If you select one, the others are disabled.

   - To select devices manually:

     a. Click the **Select Device Manually** option, if it is not selected previously.

     > **NOTE:** The **Select Device Manually** option is selected by default and the list of devices associated with the user is displayed.

     b. Select the devices on which you want to run the operation. Perform one of the following actions:

        - Select one or more devices by selecting the check box corresponding to the devices.
        - Select all devices by selecting the check box in the column header next to the **Host Name**.
        - Search for devices, or filter devices based on tags by using the search option provided.

        > **NOTE:** The search field is available only for the **Select Device Manually**. Using the search field, you can search for devices by the device name, Device Alias custom label, or tag and then select devices by clicking the corresponding check boxes.

        The total number of devices selected is displayed and dynamically updated as you select or clear the devices.

     c. (Optional) You can tag the selected devices so that you can reuse the same group of devices to run a different operation. To tag the devices, enter the name of a tag in the **Tag Selected Devices As** text box and click **Apply Tag**.

   - To select devices on the basis of tags:

a. Click the **Select by Tags** option.

   The **Select by tags** list is activated.

b. Click the arrow on the **Select by Tags** list.

   A list of public and private tags associated with the user is displayed.

   > **NOTE:** If no tags are displayed, then no devices are associated with the user's private tags or the public tags. You must tag the devices on the Device Management page for devices to be associated with tags.

c. Select the check boxes next to the name of the tag to select one or more tags. Optionally, you can filter the tags by entering the name in the text box and select the tags.

d. Click **OK**.

   The devices associated with the selected tags are displayed in the table. When you select devices based on tags, you cannot modify the list of devices displayed.

   > **NOTE:** The tags that you selected are displayed next to the **Select by Tags** field. The number of devices associated with the selected tags is also displayed

e. (Optional) An [X] icon appears after each tag name. You can use the [X] icon to clear any tag from the list. The device count in the Select Devices status bar decrements accordingly.

- To select devices by using a CSV file:

  a. Select the **Select by CSV** option.

  b. Click **Browse** and in the subsequent dialog box, select the CSV file containing the list of devices on which you want to execute the operation.

     The filename is displayed in the field next to the **Browse** button.

  c. Click **Upload**.

     The devices listed in the CSV file are displayed in the table. When you import devices using a CSV file, you cannot modify the list of devices displayed.

> **NOTE:** If you import an invalid CSV file an import failure error message is displayed. Download the sample CSV file by clicking the **View Sample CSV** link and ensure that the format of the CSV file that you are uploading is the same as the sample CSV file.

From Release 17.1R1 onward, when you upload a CSV file to select devices from, Junos Space Platform verifies the devices in the CSV file. If the CSV file contains devices to which the changes do not apply, a warning message appears which says "Few devices are not selected due to precondition failure. Please click "View inapplicable devices" for more details." You can click the View inapplicable devices link to review the list of devices that are excluded from the update.

5. (Optional) You can also schedule a time for the operation to run by selecting the **Schedule at a later time** check box and using the calendar icon and drop-down list respectively to specify the date and time when you want to run the operation.

   > **NOTE:** If you select devices based on tags and if you schedule the operation to run later, the devices associated with the tags are resolved at runtime. The operation is run only on those devices that are associated with the tags at the time of running of the operation.

6. Click **OK**.

   If you did not specify a later date and time for the operation to be run, the selected operation is executed and a dialog box appears, displaying a link to the job. Perform one of the following actions on the jobs dialog box:

   - Click the ***job ID*** link to view the status of the operation execution, and on the Job Management page, double-click the row corresponding to the job to view the details of the job.
     - If the operation was executed successfully, you can export the details of the operation as a comma-separated values (CSV) file by clicking the **Export as CSV** button and saving the file on your PC.
     - If the execution of the operation failed, the reason for the failure is displayed.
   - Click **OK** to return to the Operations page.

RELATED DOCUMENTATION

Operations Overview | 730

Creating an Operation | 731

Modifying an Operation | 740
Copying an Operation | 745
Viewing Operation Results | 744
Deleting an Operation | 748
Exporting an Operation in .tar Format | 746
Importing an Operation | 736

Viewing Operation Results

Using Junos Space Network Management Platform, you can view information about operations in the following stages of execution:

- Operations that were successfully executed
- Operations that were not successfully executed
- Operations that are currently being executed
- Operations that are scheduled to be executed later

To view information about an operation:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Operations**.

   The Operations page appears.

2. Click the **View Operation Results** icon.

   The View Operation Results page appears and displays the following information:

   - Operation name
   - Date of execution
   - Summary of the result (such as the number of devices on which the operation was successfully executed)
   - Execution status (scheduled, in progress, success, or failure)
   - Job ID

   All fields, except the Result Summary field, on the View Operation Results page have the filter option enabled. You can click the arrow on the column header of the required field to display the filter option. Select the option and specify the filter criteria. On applying the filters, the table displays only those operation results that match the filter criteria.

3. (Optional) Double-click an operation to open the **Operation Result Detail** page, which displays information about the selected operation according to device name and result (success or failed), along with a summary of the operation. Child operations are automatically expanded in the Operation Result Detail of a device. The detail is a flattened list of script or image entries.

   You can expand an individual row to view more information about the scripts, images, and child operations (operations within an operation) associated with that device. You can also expand the rows of child operations to see information about all the scripts and images associated with the operation. This way, you are able to monitor the status of each script or image associated with an operation and identify the causes of failed executions (if any).

   On the Operation Result Detail page, you can perform the following actions:

   - To view the success or failure details of individual tasks, you can click the required row.
   - To export the operation results, click **Export as CSV**. The Export as CSV page appears displaying the results in .csv format.

     To exit this page, click the **X** symbol at the top-right corner of the page. You are returned to the Operation Result Detail page.
   - Click **Close** on the Operation Result Detail page to go back to the View Operation Results page.

   You can click **Operations** in the breadcrumbs at the top of the page to return to the Operations page.

RELATED DOCUMENTATION

Operations Overview | 730

Creating an Operation | 731

Modifying an Operation | 740

Running an Operation | 740

Copying an Operation | 745

Deleting an Operation | 748

Copying an Operation

You can use Junos Space Network Management Platform to create copies of operations existing in the Junos Space Network Management Platform database.

To create a copy of an operation:

1. On the Junos Space Network Management Platform UI, select **Images and Scripts** > **Operations**.

   The **Operations** page appears, displaying the existing operations in Junos Space Network Management Platform.

2. Select the operation that you want to copy.

3. Select **Clone Operation** from the shortcut menu.

   The **Clone Operation** dialog box appears, prompting you to enter a name for the new operation.

4. Enter a name for the new operation in the **Destination Name** field.

5. Click **Clone** to create a copy of the operation.

   You are returned to the Operations page on the Junos Space UI, where you can see the new operation listed.

RELATED DOCUMENTATION

- Operations Overview | 730
- Creating an Operation | 731
- Modifying an Operation | 740
- Running an Operation | 740
- Deleting an Operation | 748
- Viewing Operation Results | 744

Exporting an Operation in .tar Format

Junos Space Network Management Platform enables you to export operations from the Junos Space Platform database to your local file system. The export operation enables you to have a local copy of the operations, which you can transfer among multiple Junos Space Platform instances for efficient use and reuse. It also allows you to make configuration changes to the operations, locally (offline). The export operation does not delete the operations that you export from the Junos Space Platform database.

The operations are exported in .tar format. The exported file does not include any objects that are referenced within the operations. For example, if an operation includes an action on an image or a script, exporting the operation does not export the referenced image or script.

To export an operation:

1. On the Junos Space Platform UI, select **Images and Scripts > Operations**.

   The Operations page appears, displaying the existing operations in Junos Space Platform.

2. Select the operations to export.

3. Select **Export Operations** from the Actions menu.

   The Export Operations page appears indicating that the selected operations will be exported in .tar format.

4. Click **OK** on the Export Operations page.

   The File Open dialog box appears and enables you to save the operation files in .tar format and the **Export Operations Job Status** dialog box displays the status of this task.

5. Click **OK** in the File Open dialog box to save the files to your local file system. Alternatively, you can save the .tar file by clicking the **Download** link in the Export Operations Job Status dialog box. If you want to view the status of the export job, click the progress bar in the Export Operations Job Status dialog box.

6. Unzip the file to view the contents.

> **NOTE:** When you export a nested operation (that is, an operation containing one or more operations), each operation is exported as a separate XML file. For example, when you export a nested operation A containing operation B and operation C, the extracted folder contains three XML files, one for each operation.

RELATED DOCUMENTATION

- Operations Overview | 730
- Creating an Operation | 731
- Modifying an Operation | 740
- Running an Operation | 740
- Copying an Operation | 745
- Viewing Operation Results | 744
- Deleting an Operation | 748

Importing an Operation | 736

Deleting an Operation

You can use Junos Space Network Management Platform to delete operations from the Junos Space Network Management Platform database.

To delete an operation:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Operations**.

   The Operations page appears, displaying the existing operations in Junos Space Network Management Platform.

2. Select the operations that you want to delete.

3. Click the **Delete Operations** icon.

   The **Delete Operations** dialog box appears, listing the operations that you chose for deletion.

4. Click **Delete** to delete the operations.

   The selected operations are deleted and you are returned to the Operations page.

> **NOTE:** When you delete an operation, you do not delete the scripts, images or operations associated with the operation from the Junos Space Network Management Platform database.

RELATED DOCUMENTATION

Operations Overview | 730
Creating an Operation | 731
Modifying an Operation | 740
Running an Operation | 740
Copying an Operation | 745
Viewing Operation Results | 744

CHAPTER 39

Managing Script Bundles

IN THIS CHAPTER

- Script Bundles Overview | 749
- Creating a Script Bundle | 750
- Viewing Script Bundles | 753
- Modifying a Script Bundle | 754
- Staging Script Bundles on Devices | 755
- Enabling Scripts in Script Bundles on Devices | 758
- Executing Script Bundles on Devices | 760
- Disabling Scripts in Script Bundles on Devices | 763
- Viewing Device Associations of Scripts in Script Bundles | 765
- Deleting Script Bundles | 765

Script Bundles Overview

Scripts are configuration and diagnostic automation tools provided by the Junos operating system (Junos OS). They help reduce network downtime and configuration complexity, automate common tasks, and reduce the time required to resolve problems. Junos OS scripts are of three types: commit, operation (op), and event scripts. For more information about scripts, see “Scripts Overview” on page 673.

Junos Space Network Management Platform allows you to group multiple op and commit scripts into a script bundle. To create a script bundle, you must first import the scripts that you want to include in the script bundle into Junos Space Platform (see “Importing Scripts to Junos Space” on page 676). The script bundles that you create are displayed on the Script Bundles page on the Junos Space UI. Script bundles can be staged and executed on devices. You can also modify and delete script bundles.

Based on the roles assigned to your username, Junos Space Platform enables or disables different tasks. For more information about the roles that you need to be assigned to perform tasks on script bundles, see “Device Images and Scripts Overview” on page 609.

You can execute the following tasks from the Script Bundles page:

- Create a script bundle.
- View details about a script bundle.
- Modify a script bundle.
- Delete script bundles.
- Execute script bundles on devices.
- Stage a script bundle on devices.
- View device association of scripts in script bundles.
- Enable scripts in a script bundle on devices.
- Disable scripts in a script bundle on devices.
- Tag and untag script bundles, view script bundles that are tagged, and delete private tags.

RELATED DOCUMENTATION

Creating a Script Bundle | **750**

Staging Script Bundles on Devices | **755**

Executing Script Bundles on Devices | **760**

Modifying a Script Bundle | **754**

Deleting Script Bundles | **765**

Enabling Scripts in Script Bundles on Devices | **758**

Disabling Scripts in Script Bundles on Devices | **763**

Viewing Device Associations of Scripts in Script Bundles | **765**

Device Images Overview | **613**

Scripts Overview | **673**

Operations Overview | **730**

Creating a Script Bundle

Junos Space Network Management Platform allows you to group multiple op and commit scripts into a script bundle. To create a script bundle, you must first import the scripts that you want to include in the script bundle into Junos Space Network Management Platform (see “Importing Scripts to Junos Space” on page 676).

To create a script bundle:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Script Bundles** and select the **Create Script Bundle** icon.

   The Create Script Bundle page appears.

2. In the **Name** text box, type the name of the script bundle.

   The script bundle name cannot exceed 50 characters. The name can contain only letters and numbers and can include a hyphen (-), underscore (_), or period (.). The name cannot start with a space.

3. In the **Description** text box, type a description of the script bundle.

   The script bundle description cannot exceed 256 characters. The description can contain only letters and numbers and can include a hyphen (-), underscore (_), period (.), or comma (,).

4. Click the **Add Scripts** ( ) icon to add scripts that need to be included in the script bundle.
   The Select Scripts page displays all Junos Space Platform scripts that you can include in the script bundle.

5. Select the scripts that you want to include in the script bundle.
   The selected scripts are highlighted.

6. (Optional) To mark scripts in the script bundle as My Favorite:
   a. Right-click the scripts and select **Mark as Favorite**.

      The Mark as Favorite pop-up window is displayed. The name of the tag is set to My Favorite and the tag is private.

   b. (Optional) In the **Description** field, enter a description.

   c. Click **Apply Tag**.

      The scripts are tagged.

7. (Optional) To unmark scripts in the script bundle that are marked as favorite:
   a. Right-click the scripts and select **Unmark as Favorite**.

      The Unmark as Favorite pop-up window that appears displays the message that the scripts are successfully unmarked as favorite.

   b. Click **OK**.

8. Click **Add**.

   The selected scripts are included in the **Selected Scripts** area of the **Create Script Bundle** page.

9. On the Create Script Bundle page, under the Selected Scripts area, you can edit the script parameters, rule, and version.

   To edit script parameters:

   a. (Optional) To change the version of the script, click the Edit icon next to the version and select a suitable version from the Version drop-down list. By default, the latest version of the script is associated with the script bundle.

   b. (Optional) You can set success or failure criteria based on the script output. When you set criteria, the script execution is considered a success or a failure only if the specified criteria are met by the execution results. By default, no specific strings are searched for in the script output and if the script is executed without any errors, then the execution is considered a success.

   c. Click **Save** to save the script parameters, rule, and version details.

10. (Optional) On this page, you can also modify the list of selected scripts by using the icons described in Table 91.

    Table 91: Create Script Bundle Page Icon Descriptions

Icon	Description
	Add scripts to the script bundle.
	Delete the selected script from the script bundle.
	Move the selected script to the row above.
	Move the selected script to the row below.
	Make a copy of the selected script and include it in the script bundle.
	Edit the value (success or failure) of script parameters or the script version. This option is disabled when commit scripts are selected.

11. Click **Save**.
    The script bundle is created and displayed on the Script Bundles page.

To verify whether the script bundle is created with your specifications, double-click the script bundle and view its details.

RELATED DOCUMENTATION

Staging Script Bundles on Devices | 755

Modifying a Script Bundle | 754

Scripts Overview | 673

Viewing Script Bundles

Junos Space Network Management Platform allows you to group multiple operation (op) and commit scripts into a script bundle. The script bundles that you create are displayed on the Script Bundles page of the Junos Space Platform UI. You can view information about all the script bundles from the Script Bundles page and you can view detailed information about a particular script bundle by using the View Script Bundle Details option.

To view script bundles from the Script Bundles page:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Script Bundles**.

   The Script Bundles page appears, displaying the script bundles created in Junos Space Platform.

   Table 92 describes the fields displayed on the Script Bundles page.

   You can use the filter option on the **Script Bundle Name** and **Domain** drop-down lists to specify the filter criteria. When you apply the filters, the page displays only the script bundles that match the filter criteria. The **Creation Date** and **Last Updated Time** fields do not support the filter option.

2. Select a script bundle and click the **View Script Bundle Details** icon, or double-click the script bundle whose details you want to view.

   The **Script Bundle Detail** dialog box appears.

   Table 92 also contains the description of fields in the Script Bundle Detail dialog box.

Table 92: Description of Fields on the Script Bundles Page and the Script Bundle Detail dialog box

Field	Description	Displayed In
Script Bundle Name	Name of the script bundle	**Script Bundles** page
Domain	Domain to which the script bundle is assigned. Default domain is Global.	**Script Bundles** page

Table 92: Description of Fields on the Script Bundles Page and the Script Bundle Detail dialog box *(continued)*

Field	Description	Displayed In
Creation Date	Date and time when the script bundle was created	**Script Bundles** page
Last Updated Time	Date and time when the script bundle was modified	**Script Bundles** page
Name	Name of the script bundle	**Script Bundle Detail** dialog box
Scripts Count	Number of scripts in the script bundle	**Script Bundle Detail** dialog box
Description	Description of the script bundle	**Script Bundle Detail** dialog box
Sequence	Sequence number of the script in the script bundle	**Script Bundle Detail** dialog box
Script Name	Name of the script in the script bundle	**Script Bundle Detail** dialog box
Descriptive Name	Descriptive name of the script that is specified using the @NAME annotation	**Script Bundle Detail** dialog box
Script Version	Version number of the script	**Script Bundle Detail** dialog box

RELATED DOCUMENTATION

Script Bundles Overview | 749

Creating a Script Bundle | 750

Modifying a Script Bundle

Junos Space Network Management Platform allows you to modify a script bundle's description, number of scripts included in the script bundle, and the script parameter value (success or failure) of every script included in the script bundle.

To modify script bundles:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Script Bundles**.

   The Script Bundles page appears, displaying all Junos Space Platform script bundles.

2. Select the script bundle that you want to modify.

3. Click the **Modify Script Bundle** icon.
   The **Modify Script Bundle** page appears.

4. Modify the necessary parameters. For more information, see "Creating a Script Bundle" on page 750.

5. Click **Modify**.

   Your modifications are saved and the Script Bundles page appears.

To verify whether your changes are saved, double-click the script bundle and view its details.

RELATED DOCUMENTATION

Staging Script Bundles on Devices | 755

Executing Script Bundles on Devices | 760

Scripts Overview | 673

Staging Script Bundles on Devices

Junos Space Network Management Platform allows you to stage script bundles on devices. During script bundle staging, op scripts and commit scripts in the script bundle are copied to the **/var/db/scripts/op** directory on the device. When you stage script bundles on dual Routing Engines, the script bundles are copied to both Routing Engines, and in case of Virtual Chassis, the script bundles are copied to all the FPCs.

To stage script bundles on devices:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Script Bundles**.

   The Script Bundles page appears, displaying all Junos Space Platform script bundles.

2. Select the script bundles that you want to stage on devices.

3. Select **Stage Script Bundle on Devices** from the Actions menu.
   The **Stage Script Bundle On Device(s)** dialog box appears.

4. Keep the **Enable Scripts on Devices** check box selected if you want the scripts to be enabled and ready to be executed when you stage them from Junos Space Platform.

   If you want the scripts to be disabled while staging them on the devices, clear this check box. However, before you run the script bundle make sure that the scripts are enabled.

5. Select the **Show existing Staged Devices** check box to display the devices on which the scripts are staged. When this check box is selected, the **Select Devices** section displays the devices on which the scripts are staged along with the devices on which the scripts are not staged.

6. Select the devices on which you want to stage the script bundles.

   You can select devices by using one of the following selection modes—manually, on the basis of tags, or by using the comma-separated values (CSV) file. These options are mutually exclusive. If you select one, the others are disabled.

   > **NOTE:** By default, the **Select Device Manually** option is selected and the list of devices on which the script bundle is not staged is displayed.

   - To select devices manually:
     - Click the **Select Device Manually** option and select the devices on which you want to stage the script bundle. The Select Devices status bar shows the total number of devices that you have selected; the status bar is dynamically updated as you select the devices.
     - To select all the devices, select the check box in the column header next to Host Name.
   - To select devices on the basis of tags:
     a. Click the **Select by Tags** option.

        The Select by tags list is activated.

     b. Click the arrow on the **Select by Tags** list.

        A list of tags defined on devices in Junos Space Platform appears, displaying two categories of tags—Public and Private.

        > **NOTE:** If no tags are displayed, then it means that none of the devices is associated with any tag. You need to tag the devices on the Device Management page before you can use the **Select by Tags** option.

c. To select tags, perform one of the following actions :

- Select the check boxes next to the tag names to select the desired tags and click **OK**.
- To search for a specific tag, enter the first few letters of the tag name in the **Select by Tags** field to the left of the **OK** button. If a match is found, a suggestion is made. Select the suggested match and click **OK**.

As you select the tags, the total number of devices associated with the selected tags appears just above the device display table. For example, if there are six devices associated with the selected tags, then **6 items selected** is displayed.

The selected tags appear next to the **Tags Selected** label. An [X] icon appears after each tag name. You can click the [X] icon to clear any tag from the list. The device count decrements accordingly.

The device display table displays the devices associated with the selected tags.

- To select devices by using a CSV file:

a. Select the **Select by CSV** option.

b. Click **Browse** to navigate to the file location on your computer and select the CSV file containing the list of devices on which you want to stage the script bundle.

> **TIP:** For a sample CSV file, click the **Sample CSV** link. You are prompted to save the file. Save the file to your computer and open it by using an application such as Microsoft Excel.

c. Click **Upload** to upload the CSV file.

From Release 17.1R1 onward, when you upload a CSV file to select devices from, Junos Space Platform verifies the devices in the CSV file. If the CSV file contains devices to which the changes do not apply, a warning message appears which says "Few devices are not selected due to precondition failure. Please click "View inapplicable devices" for more details." You can click the View inapplicable devices link to review the list of devices that are excluded from the update.

7. (Optional) To schedule a time for staging the script bundles, select the **Schedule a later time** check box and use the calendar icon and drop-down list respectively to specify the date and time when you want the script bundles to be staged.

8. Click **Stage**.

The selected script bundles are staged and a Jobs dialog box appears displaying a job ID link. Perform one of the following actions in the Jobs dialog box:

- Click the ***job ID*** link to view the status of the staging operation on the Job Management page. If the staging of the script bundles fails, you can identify the reason for failure by double-clicking the job on the Job Management page. The Job Details page appears and displays the reason for failure in the Description column. The Job Details page supports sorting of data in all columns in ascending or descending order.
- Click **OK** to return to the Script Bundles page.

To return to the Script Bundles page from anywhere on the Junos Space Platform UI, select **Images and Scripts** > **Script Bundles** on the left pane of the UI.

RELATED DOCUMENTATION

Creating a Script Bundle | **750**

Modifying a Script Bundle | **754**

Deleting Script Bundles | **765**

Executing Script Bundles on Devices | **760**

Enabling Scripts in Script Bundles on Devices | **758**

Disabling Scripts in Script Bundles on Devices | **763**

Script Bundles Overview | **749**

Enabling Scripts in Script Bundles on Devices

After you stage the script bundle, you can use Junos Space Network Management Platform to enable the scripts within the script bundle on one or more devices simultaneously.

To enable the scripts on devices:

1. On the Junos Space Network Management Platform UI, select **Images and Scripts > Script Bundles**.

   The Script Bundles page appears, displaying all Junos Space Network Management Platform script bundles.

2. Select the script bundle containing the scripts that you want to enable on devices.

3. Select **Enable Script Bundle on Devices** from the Actions menu. If this option is unavailable, it means that one or more of the scripts within the script bundle are not staged on any of the devices. You must first stage the scripts and then enable them.

The Enable Script Bundle On Device(s) page appears. However, if all the scripts within the script bundle are enabled on all the associated devices, then Junos Space Network Management Platform displays the following message indicating that there are no scripts that can be enabled.

No devices found where all the scripts of the selected bundle are staged and at least one script is disabled

> **NOTE:** The Enable Script Bundle On Device(s) page lists those devices that are associated with all scripts (enabled or disabled) in the script bundle. However, devices are not listed in the following cases:
>
> - If the script version in the script bundle does not match the staged version of the script on the devices
> - If all scripts in the script bundle are enabled on the devices
> - If a device-script association does not exist on the device for at least one script (enabled or disabled) in the script bundle

4. Select the devices on which you want the script bundle to be enabled.

5. Click **Enable**.

   The scripts within the script bundle are enabled on the selected devices and a Jobs dialog box displays a job ID link. Perform one of the following actions:

   - Click the ***job ID*** link to view the job status on the Job Management page. If the scripts are not enabled on the selected devices, you can identify the reason for failure by double-clicking this job on the Job Management page. The Job Details page appears and displays the reason for failure in the Description column.
   - Click **OK** to return to the Scripts Bundles page.

To return to the Script Bundles page from anywhere on the Junos Space Platform GUI that you may have navigated to, select **Images and Scripts** > **Script Bundles** on the left pane of the GUI.

RELATED DOCUMENTATION

Disabling Scripts in Script Bundles on Devices | 763

Creating a Script Bundle | 750

Modifying a Script Bundle | 754

Deleting Script Bundles | 765

Staging Script Bundles on Devices | 755

Executing Script Bundles on Devices | 760
Script Bundles Overview | 749

Executing Script Bundles on Devices

Junos Space Network Management Platform allows you to execute script bundles on devices. When you execute script bundles, Junos Space Platform triggers the execution of op scripts on the selected devices. Commit scripts are executed on commit when events occur on the device and therefore the result of the script bundle execution for commit scripts is always shown as Success in Junos Space Platform.

To execute script bundles on devices:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Script Bundles**.

   The Script Bundles page appears, displaying all Junos Space Platform script bundles.

2. Select the script bundles that you want to execute on devices.

3. Right-click your selection or use the Actions menu, and select **Execute Script Bundle on Devices**. The **Execute Script Bundle On Device(s)** dialog box appears.

   To restage the scripts before execution, keep the **Stage & Enable Scripts before Execution** check box selected (the default). If the scripts within the script bundle are previously staged and enabled in all the necessary devices and you do not want to restage these scripts, clear this check box.

4. Select the devices on which you want to execute the scripts.

   You can select devices by using one of the following selection modes—manually, on the basis of tags, or by using the CSV file. These options are mutually exclusive. If you select one, the others are disabled.

   > **NOTE:** By default, the **Select Device Manually** option is selected and the list of devices on which the scripts in the script bundle are staged and enabled is displayed.

   - To select devices manually:
     - Click the **Select Device Manually** option and select the devices on which you want to execute the scripts in the script bundle. The Select Devices status bar shows the total number of devices that you have selected; the status bar is dynamically updated as you select the devices.
     - To select all the devices, select the check box in the column header next to Host Name.
   - To select devices on the basis of tags:

a. Click the **Select by Tags** option.

   The Select by Tags list is activated.

b. Click the arrow on the **Select by Tags** list.

   A list of tags defined on devices in Junos Space Platform appears, displaying two categories of tags—Public and Private.

   > **NOTE:** If no tags are displayed, then it means that none of the devices is associated with any tag. You need to tag the devices on the Device Management page before you can use the **Select by Tags** option.

c. To select tags, perform one of the following actions :

   - Select the check boxes next to the tag names to select the desired tags and click **OK**.
   - To search for a specific tag, enter the first few letters of the tag name in the **Select by Tags** field to the left of the **OK** button. If a match is found, a suggestion is made. Select the suggested match and click **OK**.

   As you select the tags, the total number of devices associated with the selected tags appears just above the device display table. For example, if there are six devices associated with the selected tags, then **6 items selected** is displayed.

   The selected tags appear next to the **Tags Selected** label. An [X] icon appears after each tag name. You can click the [X] icon to clear any tag from the list. The device count decrements accordingly.

   The device display table displays the devices associated with the selected tags.

- To select devices by using a CSV file:

  a. Select the **Select by CSV** option.

  b. Click **Browse** to navigate to the file location on your computer and select the CSV file containing the list of devices on which you want to execute the script bundle.

     > **TIP:** For a sample CSV file, click the **Sample CSV** link. You are prompted to save the file. Save the file to your computer and open it by using an application such as Microsoft Excel.

  c. Click **Upload** to upload the CSV file.

From Release 17.1R1 onward, when you upload a CSV file to select devices from, Junos Space Platform verifies the devices in the CSV file. If the CSV file contains devices to which the changes do not apply, a warning message appears which says "Few devices are not selected due to precondition failure. Please click "View inapplicable devices" for more details." You can click the View inapplicable devices link to review the list of devices that are excluded from the update.

5. (Optional) You can modify the script parameters before executing script bundles on devices. The changes made to script parameters are saved only on the devices on which the script bundle is executed. The script parameters in the script bundle in Junos Space Platform continue to reflect the original values.

   To edit the script parameter values before execution:

   1. On the Execute Script Bundle On Device(s) page, click the **Update Script Parameters/Rule** link.

      The **Configure Script Bundle Parameters** dialog box appears.

   2. Click **set value** to edit the script parameters and click **Save**.

      You can also set success or failure criteria based on the script output. When you set criteria, the script execution is considered a success or a failure only if the specified criteria (text string) is present in the execution results. By default, no specific strings are searched in the script output and if the script is executed without any errors, then the execution is considered a success.

   3. Click **Configure**. Your changes are saved and the **Enable Script Bundle On Device(s)** dialog box displays your previous selections.

6. (Optional) To schedule a time for executing the script bundles, select the **Schedule a later time** check box and use the calendar icon and drop-down list respectively to specify the date and time when you want the script bundles to be executed.

7. Click **Execute**.
   The script bundle is enabled and executed on the selected devices and a Jobs dialog box displays a job ID link. Perform one of the following actions in the Jobs dialog box:

   - Click the ***job ID*** link to view the status of execution on the Job Management page. If the execution of the script bundles fails, you can identify the reason for failure by double-clicking this job on the Job Management page. The Job Details page appears and displays the reason for failure in the Description column. The Job Details page supports sorting of data in all columns in ascending or descending order.
   - Click **OK** to return to the Script Bundles page.

To return to the Script Bundles page from anywhere on the Junos Space Platform UI, select **Images and Scripts** > **Script Bundles** on the left pane of the UI.

RELATED DOCUMENTATION

Creating a Script Bundle | 750
Modifying a Script Bundle | 754
Deleting Script Bundles | 765
Staging Script Bundles on Devices | 755
Enabling Scripts in Script Bundles on Devices | 758
Disabling Scripts in Script Bundles on Devices | 763
Script Bundles Overview | 749

Disabling Scripts in Script Bundles on Devices

You can disable the scripts in a script bundle on devices on which they are in the enabled state. You can use Junos Space Network Management Platform to disable the scripts within the script bundle on one or more devices simultaneously.

To disable the scripts on devices:

1. On Junos Space Platform, select **Images and Scripts > Script Bundles**.

   The Script Bundles page appears, displaying all Junos Space Platform script bundles.

2. Select the script bundle containing the scripts that you want to disable on devices.

3. Select **Disable Script Bundle on Devices** from the Actions menu. If this option is unavailable, it means that one or more of the scripts within the script bundle is not staged on a device.

   The Disable Script Bundle On Device(s) page appears, which displays the devices on which the scripts are staged and enabled. However, if all the scripts within the script bundle are already disabled, then Junos Space Platform displays the following message indicating that there are no scripts that can be disabled.

   No devices found where all the scripts of the selected bundle are staged and at least one script is enabled

NOTE:

The Disable Script Bundle On Device(s) page lists the devices that are associated with the same versions of all scripts that are part of the script bundle. The scripts might be in an enabled or disabled state.

This page does not list devices:

- If the script version in the script bundle does not match the staged version of the script on the devices.
- If all the scripts in the script bundle are in a disabled state on the devices.
- If a device-script association does not exist on the device for at least one script (in an enabled or disabled state) in the script bundle.

4. Select the devices on which you want the scripts to be disabled.

5. Click **Disable**.

   The scripts within the script bundle are disabled on the selected devices and a Jobs dialog box displays a job ID link. Perform one of the following actions on the Jobs dialog box:

   - Click the ***job ID*** link to view the job status on the Job Management page. If the scripts are not disabled on the selected devices, you can identify the reason for failure by double-clicking this job on the Job Management page. The Job Details page appears and displays the reason for failure in the Description column. The Job Details page supports sorting of data in all columns in ascending or descending order.
   - Click **OK** to return to the Script Bundles page.

To return to the Script Bundles page from anywhere on the Junos Space Platform UI, select **Images and Scripts** > **Script Bundles** on the left pane of the UI.

RELATED DOCUMENTATION

Enabling Scripts in Script Bundles on Devices | **758**

Viewing Device Associations of Scripts in Script Bundles | **765**

Modifying a Script Bundle | **754**

Deleting Script Bundles | **765**

Staging Script Bundles on Devices | **755**

Executing Script Bundles on Devices | **760**

Script Bundles Overview | **749**

Viewing Device Associations of Scripts in Script Bundles

You can view the devices on which the scripts from a script bundle are staged by using the View Associated Devices option from the Actions menu in Junos Space Network Management Platform.

To view the scripts and their associated devices:

1. On the Junos Space Platform UI, select **Images and Scripts > Script Bundles**.

   The Script Bundles page appears, displaying all Junos Space Platform script bundles.

2. Select the script bundles for which you want to view device associations.

3. Select **View Associated Devices** from the Actions menu.

   The View Associated Devices page appears, displaying the scripts (Script Name column) and the devices (Host Name and IP Address columns) with which they are associated along with other details, such as the latest version of the script, script type, staged version of the script, platform of the device, software version running on the device, activation status of the script and the script bundle, and the domain to which they belong.

4. Click **Back** to go back to the Script Bundles page.

RELATED DOCUMENTATION

- Enabling Scripts in Script Bundles on Devices | **758**
- Disabling Scripts in Script Bundles on Devices | **763**
- Modifying a Script Bundle | **754**
- Deleting Script Bundles | **765**
- Staging Script Bundles on Devices | **755**
- Executing Script Bundles on Devices | **760**
- Script Bundles Overview | **749**

Deleting Script Bundles

Junos Space Network Management Platform enables you to delete multiple script bundles simultaneously.

To delete script bundles:

1. On the Junos Space Platform UI, select **Images and Scripts** > **Script Bundles**.

   The Script Bundles page appears, displaying all Junos Space Platform script bundles.

2. Select the script bundles that you want to delete.

3. Select the **Delete Script Bundles** icon.

   The **Delete Device Script Bundles** dialog box appears and displays the names of the selected script bundles.

4. Click **Delete** to confirm that you want to delete the selected script bundles.

   The Jobs dialog box appears, displaying a job ID link. Perform one of the following actions on the Jobs dialog box:

   - Click the ***job ID*** link to view the status of the delete operation on the Job Management page. If the deletion of the script bundles fails, you can identify the reason for failure by double-clicking this job on the Job Management page. The Job Details page appears, displaying the reason for failure in the Description column. The Job Details page supports sorting of data in all columns in ascending or descending order.
   - Click **OK** to return to the Scripts Bundles page.

If the script bundles are successfully deleted, then the deleted script bundles are not listed on the Script Bundles page.

RELATED DOCUMENTATION

Creating a Script Bundle | 750

Executing Script Bundles on Devices | 760

Scripts Overview | 673

6

PART

Reports

Reports Overview | **768**

Report Definitions | **780**

Reports | **788**

CHAPTER 40

Reports Overview

IN THIS CHAPTER

- Reports Overview | 768

Reports Overview

IN THIS SECTION

- Audit Trail Report Type | 770
- Device Inventory Report Type | 770
- Device License Inventory Report Type | 771
- Device Logical Interface Inventory Report Type | 772
- Device Physical Interface Inventory Report Type | 774
- Device Physical Inventory Report Type | 775
- Device Software Inventory Report Type | 776
- Job Inventory Report Type | 777
- User Account Report Type | 778

You can use the Reports workspace to generate customized reports for managing the resources on your network. You can use these reports to gather device inventory details, job execution details, and audit trails.

You first create a report definition to specify what information to retrieve from the Junos Space Network Management Platform inventory database. You then use this report definition to generate, export, and print the reports. Junos Space Network Management Platform provides some predefined categories (report types) to create report definitions.

You combine multiple report types to create a report definition; you can also create a report definition using one report type. By default, a predefined set of attributes is included in a report type. You can choose

to add or remove the attributes in a report type according to what information you want from the final generated report. You can group, sort, or filter data by using specific attributes in each report type.

You can apply multiple filter criteria to columns in a report type to filter data. For example, you can filter a User Accounts report type by roles, user type, and GUI or API access. From Junos Space Network Management Platform Release 16.1R1 onward, you can filter columns by domains also. You can separate the filter criteria with commas. Columns that meet the filter criteria are listed in the report generated from the report definition. The data types that support filtering using multiple filter values are String, Integer, Date, and Enum.

You can use the report definitions to generate reports in CSV, HTML, and PDF formats. The reports display the name and description of the report. You can schedule the delivery of generated reports to a designated SMTP server or an SCP server. You can view, download, or print the generated reports from the Generated Reports page in the Reports workspace. You can also tag the reports and report definitions. For more information, see “Tagging an Object” on page 1526.

> **NOTE:** Reports generated in a parent domain include information from all subdomains. Reports generated in a subdomain include information from only that subdomain. The reports that you generate can contain information from all accessible domains if you set the "Manage objects from all assigned domains” flag as your preference. To set this flag, click the **User Settings** icon on the Junos Space banner and click the **Object Visibility** tab.

You need to be assigned the necessary privileges to generate reports for a specific type of report in a report definition. Table 93 displays the mapping between report types and the privileges you need to be able to create, modify, or delete a report definition or view, generate, or delete reports by using the report definition.

Table 93: Privileges Required to Generate Reports for Specific Report Definition Categories

Report Types	Privileges Required to Generate Reports
Audit Trail	View Audit Logs
Device Inventory	Device Management task group
Device Physical Inventory	View Physical Inventory
Device Physical Interface Inventory	View Physical Interfaces
Device Logical Interface Inventory	View Logical Interfaces
Device License Inventory	View License Inventory

Table 93: Privileges Required to Generate Reports for Specific Report Definition Categories *(continued)*

Report Types	Privileges Required to Generate Reports
Device Software Inventory	View Software Inventory
Job Inventory	View Jobs
User Accounts	User Accounts task group

You can include the following type of reports in a report definition:

Audit Trail Report Type

This type of report enables you to view the audit log activities and tasks initiated on Junos Space Platform. Table 94 lists the attributes available with this type of report.

Table 94: Audit Trail Report Attributes

Attribute	Description
User Name	Username of the user who initiated the task
User IP	IP address of the client computer that the user used to initiate the task
Task	Name of the task that triggered the audit log
Timestamp	Time in the UTC time format in the database that is mapped to the local time zone of the client computer
Result	Execution result of the task that triggered the audit log
Job ID	Job ID of the job-based task that is included in the audit log
Description	Description of the audit log logged on Junos Space Network Management Platform
Application	Application from which the audit trail was generated

Device Inventory Report Type

This type of report enables you to view the generic characteristics of all devices managed by Junos Space Network Management Platform. Table 95 lists the attributes available with this type of report.

Table 95: Device Inventory Report Attributes

Attribute	Description
Name	Name of the device
Device Alias	Value of the Device Alias custom label for the device
Configuration State	State of the configuration on a device
Vendor	Vendor of the device
IP Address	IP address of the device
Managed Status	Current status of the managed device in Junos Space Network Management Platform
Device Family	Device family of the selected device
OS Version	Operating system firmware version running on the device
Platform	Model number of the device
Connection Status	Connection status of the device: UP or DOWN
Schema Version	Junos OS configuration schema version on the device
Authentication Status	Authentication mode and status of the device connected to Junos Space Network Management Platform: key-based, credentials-based, or key conflict
Serial Number	Serial number of the device
Connection Type	Type of connection between the device and Junos Space Network Management Platform
Domain Name	Domain to which the device is assigned

Device License Inventory Report Type

This type of report enables you to view the generic characteristics of the device license information of devices managed by Junos Space Network Management Platform. Table 96 lists the attributes available with this type of report.

Table 96: Device License Inventory Report Attributes

Attribute	Description
Device Name	Name of the device
Device Alias	Value of the Device Alias custom label for the device
Feature Name	Name of the licensed SKU or feature
License Count	Number of times an item has been licensed
Used Count	Number of times the feature is used
Need Count	Number of times the feature is used without a license
Given	Number of instances of the feature that are provided by default
OS Version	Operating system firmware version running on the device
Device Family	Device family of the selected device
Platform	Model number of the device
Serial Number	Serial number of the device

NOTE: Juniper Networks devices require a license to activate the feature. To understand more about Junos Space Network Management Platform Licenses, see, Licenses for Network Management. Please refer to the Licensing Guide for general information about License Management. Please refer to the product Data Sheets for further details, or contact your Juniper Account Team or Juniper Partner.

Device Logical Interface Inventory Report Type

This type of report enables you to view the generic characteristics of the logical interface of devices managed by Junos Space Network Management Platform. Table 97 lists the attributes available with this type of report.

Table 97: Device Logical Interface Inventory Report Attributes

Attribute	Description
Device Name	Name of the device
Device Alias	Value of the Device Alias custom label for the device
Physical Interface	Name of the physical interface
Admin Status	Administrative status of the interface: UP or DOWN
Link Type	Type of the physical interface link: full duplex or half duplex
Logical Interface	Name of the logical interface
Logical Interface IP	IP address of the logical interface
Logical Encapsulation	Encapsulation used on the logical interface
VLAN	VLAN ID of the logical interface
OS Version	Operating system firmware version running on the device
Device Family	Device family of the selected device
Platform	Model number of the device
Serial Number	Serial number of the device chassis
Device IP Address	IP address of the device
Physical Interface IP	IP address of the physical interface
MAC Address	MAC address of the physical interface
Operation Status	Operation status of the interface: UP or DOWN
Physical Encapsulation	Encapsulation used on the physical interface
Speed	Speed at which the interface is running (in Mbps)
MTU	Size of the MTU
Description	Description of the logical interface

Table 97: Device Logical Interface Inventory Report Attributes *(continued)*

Attribute	Description
IPv6 address	IPv6 address of the logical interface

Device Physical Interface Inventory Report Type

This type of report enables you to view the generic characteristics of the physical interface of devices managed by Junos Space Network Management Platform. Table 98 lists the attributes available with this type of report.

Table 98: Device Physical Interface Inventory Report Attributes

Attribute	Description
Device Name	Name of the device
Device Alias	Value of the Device Alias custom label for the device
Physical Interface	Name of the physical interface
Admin Status	Administrative status of the interface: UP or DOWN
Link Type	Type of the physical interface link: full duplex or half duplex
Link Level Type	Type of the link level
IP Address	IP address of the physical interface
OS Version	Operating system firmware version running on the device
Device Family	Device family of the selected device
Platform	Model number of the device
Serial Number	Serial number of the device chassis
MAC Address	MAC address of the physical interface
Operation Status	Operation status of the interface: UP or DOWN
Encapsulation	Encapsulation used on the physical interface
Speed	Speed at which the interface is running (in Mbps)

Table 98: Device Physical Interface Inventory Report Attributes *(continued)*

Attribute	Description
MTU	Size of the MTU
Description	Description of the physical interface
IPv6 address	IPv6 address of the physical interface

Device Physical Inventory Report Type

This type of report enables you to view the generic characteristics of the hardware modules of devices managed by Junos Space Network Management Platform. Table 99 lists the attributes available with this type of report.

Table 99: Device Physical Inventory Report Attributes

Attribute	Description
Device Name	Name of the device
Chassis	Chassis component of the device
Module	Components contained in the chassis
Sub Module	Components contained in the submodule
Sub Sub Module	Components contained in the submodule of the submodule
Sub Sub Sub Module	Components contained in the submodule of the submodule of the submodule
Model	Model name of the component
Model Number	Model number of the device component
Part Number	Part number of the chassis component
Revision	Revision number of the component
Part Serial Number	Hardware serial number of the component
Status	Current operation status of the component

Table 99: Device Physical Inventory Report Attributes *(continued)*

Attribute	Description
IP Address	IP address of the physical component
Device Family	Device family of the selected device
Platform	Model number of the device
Serial Number	Serial number of the device chassis
Description	Description of the physical component
OS Version	Operating system firmware version running on the device

NOTE: You can filter the columns in the device physical inventory report by using only tags. You can also sort and group the Device Name column only in the device physical inventory report.

Device Software Inventory Report Type

This type of report enables you to view the generic software package installation information of devices managed by Junos Space Network Management Platform. Table 100 lists the attributes available with this type of report.

Table 100: Device Software Inventory Report Attributes

Attribute	Description
Device Name	Name of the device
Package Name	Name of the software package installed on the device
Version	Version number of the software package installed on the device
Type	Type of the software package installed on the device
OS Version	Operating system firmware version running on the device
Device Family	Device family of the selected device

Table 100: Device Software Inventory Report Attributes *(continued)*

Attribute	Description
Platform	Model number of the device
Serial Number	Serial number of the device chassis
Model	Model name of the device
Routing Engine	Specific Routing Engine on the device supporting multiple Routing Engines
Description	Description of the installed software package

Job Inventory Report Type

This type of report enables you to view the generic execution characteristics of Junos Space Network Management Platform jobs. Table 101 lists the attributes available with this type of report.

Table 101: Job Inventory Report Attributes

Attribute	Description
ID	Numerical ID of the job
Name	Name of the job appended with the job ID
Percent	Percentage of completion of the job
Job Type	Supported job types
State	State of job execution
Summary	Operations executed for the job
Scheduled Start Time	Start time specified for the job
User	Username of the user who scheduled the job
Recurrence	Recurrence of the job
Retry Group ID	Job ID of the retry job
Actual Start Time	Time when the job started to execute

Table 101: Job Inventory Report Attributes *(continued)*

Attribute	Description
End Time	Time the job ended
Previous Retry	Job ID of the previous retry job
Job Parameters	Details of the objects on which the job is executed. For example, IP addresses of the devices that are discovered through a device discovery job.

User Account Report Type

This type of report enables you to view details of the user accounts in Junos Space Platform. Table 102 lists the attributes available with this type of report.

Table 102: User Account Report Attributes

Attribute	Description
User Name	Username of the user
First Name	First name of the user
Last Name	Last name of the user
Email	E-mail address of the user
User Type	Type of user: local or remote
Status	Status of the user
Password Status	Status of the password
GUI/API Access	Type of access: GUI, API, or Both
Locked Out	Whether the user is locked out
Roles	Roles assigned to the user
Domains	Domains to which the user is assigned

Release History Table

Release	Description
16.1R1	From Junos Space Network Management Platform Release 16.1R1 onward, you can filter columns by domains also.

RELATED DOCUMENTATION

- Creating Report Definitions | **780**
- Generating Reports | **789**
- Viewing Report Definition Statistics | **787**

CHAPTER 41

Report Definitions

IN THIS CHAPTER

- Creating Report Definitions | 780
- Viewing Report Definitions | 783
- Modifying Report Definitions | 784
- Cloning Report Definitions | 785
- Deleting Report Definitions | 786
- Viewing Report Definition Statistics | 787

Creating Report Definitions

Report definitions specify what information to retrieve from the Junos Space Network Management Platform inventory database and how this information is displayed in the generated reports. You can create report definitions from the Reports workspace. The Report Definitions page in the Reports workspace lists all the report definitions you created. It also lists the name of the report definition, user who created the report definition, time the report definition was created, and description of the report definition.

NOTE: The privileges assigned to you determine which types of report are available to you during this workflow. For example, if you do not have the privileges to view audit logs, the Audit Trail report type is not displayed in the report definition. For information about the mapping of types of report to the privileges you require, see "Reports Overview" on page 768.

To create a report definition:

1. On the Junos Space Network Management Platform user interface, select **Reports** > **Report Definitions**.

   The Report Definitions page that appears displays all the report definitions in the Junos Space Network Management Platform database.

2. Click the **Create Report Definition** icon on the toolbar.

   The Create Report Definition page is displayed.

3. In the **Report Name** field, type a user-defined report definition name.

   A report definition name cannot exceed 128 characters and can contain only letters, numbers, spaces, and some special characters. The special characters allowed are hyphen (-), underscore (_), period (.), at (@), forward slash (/), and ampersand (&).

   > **NOTE:** Single quotation mark (') is not allowed in the report name definition.

4. (Optional) In the **Description** field, type a user-defined description.

   The description cannot exceed 512 characters and can contain only letters, numbers, spaces, and some special characters. The special characters allowed are hyphen (-), underscore (_), period (.), at (@), single quotation mark ('), forward slash (/), and ampersand (&).

5. Click the **Add** icon below the Description field.

   The Select Report Type window is displayed.

6. Select the check boxes next to the types of report you want to add to the report definition.

7. Click **Add**.

   The types of reports you selected are added to the report definition.

8. (Optional) You can modify, filter, group, or sort the data in your report definition. To do so:

    a. Click the **Edit Columns/Filter** icon in the Filter column corresponding to the type of report in which you want to add the column and filter.

    The Edit Columns/Filters window is displayed.

    b. Select the columns that you want to add to the type of report from the Available column and click the right arrow to move the filters to the Selected column.

    c. Select an appropriate option on the **Group By** drop-down list to group the columns in the type of report in a specific order.

    d. Select an appropriate option on the **Sort By** drop-down list to sort the columns in the type of report in a specific order.

    e. Select the appropriate option button next to the Sorting Order section to choose the order of columns in the type of report.

    f. (Optional) Click the **Add Filter Criteria** icon to add filters to the type of report.

    For example, you can filter a Device Inventory report type by vendor, IP address, connection status, and domain name.

        i. Select the appropriate column from the drop-down list for which you want to add a filter.

        ii. Select the appropriate operand corresponding to the column, from the drop-down list.

        iii. Type the criteria to be filtered next to the operand.

    > **NOTE:** If you select domain as filter criteria, all domains applicable to the report type are listed. You can select multiple domains by selecting the check boxes next to the domains.

    g. To delete the filter criteria, click the **Delete** icon.

    h. Click **OK**.

    You are redirected to the Create Report Definition page.

9. (Optional) Repeat step 8 to add filters to all types of reports you selected.

10. Click **Save**.

    You are redirected to the Report Definitions page. You can use the report definition to generate reports.

    NOTE: You can view the reports generated from a report definition by clicking the View link in the Reports column corresponding to the report definition.

RELATED DOCUMENTATION

- Reports Overview | 768
- Modifying Report Definitions | 784
- Deleting Report Definitions | 786
- Generating Reports | 789

Viewing Report Definitions

You can view details of report definitions on the Report Definitions page. The Report Definitions page lists the name of the report definition, user who created the report definition, time the report definition was created, and description of the report definition.

To view details of a report definition:

1. On the Junos Space Network Management Platform user interface, select **Reports** > **Report Definitions**.

2. Select the check box next to the report definition whose details you want to view and click the View Report Definition icon on the toolbar.

   The View Report Definition window is displayed.

   You can view the types of report you selected for this report definition, the columns selected in the report type, and the filter criteria you specified.

3. Click **OK** to close the window.

RELATED DOCUMENTATION

- Reports Overview | 768

Creating Report Definitions | 780

Modifying Report Definitions

You can modify the report definitions from the Report Definitions page. The Report Definitions page lists the name of the report definition, user who created the report definition, time the report definition was created, and description of the report definition.

> **NOTE:** You cannot modify a report definition if the report definition contains a type of report that you do not have access to. The following error message is displayed if you try to modify such a report definition: **The selected report definition contains object categories that you cannot access and hence cannot be modified.** For information about the mapping of report definition categories to the privileges you require, see "Reports Overview" on page 768.

To modify a report definition:

1. On the Junos Space Network Management Platform user interface, select **Reports** > **Report Definitions**.

   The Report Definitions page that appears displays all the report definitions in the Junos Space Network Management Platform database.

2. Select the check box next to the report definition you want to modify and click the **Modify Report Definition** icon on the toolbar.

   The Modify Report Definition page is displayed. You can change all the parameters of the report definition except the name of the report definition.

3. Modify the necessary fields and click **Save**.

   The report definition is modified. You are redirected to the Report Definitions page.

RELATED DOCUMENTATION

Reports Overview | 768

Deleting Report Definitions | 786

Cloning Report Definitions | 785

Viewing Report Definitions | 783

Cloning Report Definitions

You can clone the report definitions from the Report Definitions page. The Report Definitions page lists the name of the report definition, user who created the report definition, time the report definition was created, and description of the report definition.

> **NOTE:** You cannot clone a report definition if the report definition contains a type of report that you do not have access to. The following error message is displayed if you try to clone such a report definition: **The selected report definition contains object categories that you cannot access and hence cannot be modified.** For information about the mapping of report definition categories to the privileges you require, see "Reports Overview" on page 768.

To clone a report definition:

1. On the Junos Space Network Management Platform user interface, select **Reports** > **Report Definitions**.
2. Right-click the report definition you want to clone and select **Clone Report Definition**.

   The Clone Report Definitions page is displayed.
3. In the **Report Name** field, type a user-defined report definition name.

   A report definition name cannot exceed 128 characters and can contain only letters, numbers, spaces, and some special characters. The special characters allowed are hyphen (-), underscore (_), period (.), at (@), single quotation mark ('), forward slash (/), and ampersand (&).
4. (Optional) In the **Description** field, type a user-defined description.

   The description cannot exceed 512 characters and can contain only letters, numbers, spaces, and some special characters. The special characters allowed are hyphen (-), underscore (_), period (.), at (@), single quotation mark ('), forward slash (/), and ampersand (&).
5. (Optional) Modify the types of reports included in the report definition and the respective filters.
6. Click **Clone**.

   You are redirected to the Report Definitions page.

RELATED DOCUMENTATION

Reports Overview | 768

Creating Report Definitions | 780

Deleting Report Definitions

You can delete the report definitions from the Report Definitions page. The Report Definitions page lists the name of the report definition, user who created the report definition, time the report definition was created, and description of the report definition.

> **NOTE:** You cannot delete a report definition if the report definition contains a type of report that you do not have access to. The following error message is displayed if you try to delete such a report definition: **The selected report definition contains object categories that you cannot access and hence cannot be deleted.** For information about the mapping of report definition categories to the privileges you require, see "Reports Overview" on page 768.

To delete a report definition:

1. On the Junos Space Network Management Platform user interface, select **Reports** > **Report Definitions**.

   The Report Definitions page that appears displays all the report definitions in the Junos Space Network Management Platform database.

2. Select the check boxes next to the report definitions you want to delete and click the **Delete Report Definition** icon on the toolbar.

   The Delete Report Definition window is displayed.

3. Click **Delete**.

   The report definitions are deleted. You are redirected to the Report Definitions page.

RELATED DOCUMENTATION

Reports Overview | 768

Creating Report Definitions | 780

Cloning Report Definitions | 785

Viewing Report Definitions | 783

Viewing Report Definition Statistics

You can view report definition statistics when you select the Reports workspace. The Report Definition Count by User bar chart presented on the Reports page displays the number of report definitions created per user. The chart is interactive.

To view report definition statistics:

1. On the Junos Space Network Management Platform user interface, select **Reports**.

   The Reports page is displayed. This page displays the charts related to reports and report definitions.

2. Click a specific label on the Report Definition Count by User chart.

   You are redirected to the Report Definitions page whose contents are filtered based on the label you clicked.

   To save a chart as an image or to print the chart, right-click the chart and select Save or Print respectively.

RELATED DOCUMENTATION

Reports Overview | **768**

Creating Report Definitions | **780**

Deleting Report Definitions | **786**

CHAPTER 42

Reports

IN THIS CHAPTER

- Generating Reports | **789**
- Viewing a Report | **792**
- Viewing and Downloading Generated Reports | **794**
- Deleting Generated Reports | **795**
- Viewing Report Statistics | **795**

Generating Reports

You can generate reports from the report definitions you created. You can generate the following types of reports:

- Audit Trail report
- Device Inventory report
- Device Licence Inventory report
- Device Logical Interface Inventory report
- Device Physical Interface Inventory report
- Device Physical Inventory report
- Device Software Inventory report
- Job Inventory report
- User Accounts report

> **NOTE:** You cannot generate a report if the report definition you select contains a type of report that you do not have access to. The following error message is displayed if you try to generate such a report: **The selected report definition contains object categories that you cannot access and hence cannot be used to generate report.** For information about the mapping of report definition categories to the privileges you require, see "Reports Overview" on page 768.

To generate reports:

1. On the Junos Space Network Management Platform user interface, select **Reports** > **Report Definitions**.

   The Report Definitions page that appears displays all the report definitions in the Junos Space Platform database.

2. Select the check box next to the report definition that you want to use to create a report and click the Generate Report icon on the toolbar.

   The Generate Reports window is displayed.

3. Select the report formats you want to generate by selecting the appropriate check boxes next to the Report Format field.

   Junos Space Platform provides reports in CSV, HTML, and PDF formats.

4. (Optional) Select the **SCP Server** check box to configure Junos Space Platform to store the report in a directory on a Secure Copy Protocol (SCP) server.

   To configure the SCP server:

   a. In the **IP Address** field, enter the IP address of the SCP server.

   NOTE:
   - If Junos Space fabric is configured for IPv4 only, you can enter an IPv4 address. If Junos Space fabric is configured for both IPv4 and IPv6, you can enter either an IPv4 or an IPv6 address.
   - The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to http://www.iana.org/assignments/ipv4-address-space for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space for the list of restricted IPv6 addresses.

   b. From the **Port** spin box, select the appropriate port number. By default, the port number is 22.

   c. In the **Directory** field, enter the name of the directory on the SCP server to which you want to save the reports.

   d. In the **User Name** field, enter the username that you use to access the SCP server.

e. You can select the authentication mode for saving reports to SCP server from Junos Space Network Management Platform Release 17.1R1 onward.

- To use the password mode, in the **Password** field, enter the password used to access the SCP server. By default, the **Password** mode is selected.

- To use a key generated from Junos Space Platform, click **Space Key**. Click the **Download Space Key** link to download the key.

  > **NOTE:** Alternatively, you can download the Space Key by selecting **Administration** > **Fabric** and clicking the Manage Space SSH Key icon.
  >
  > After downloading the Space Key, log in to the SCP server and append the contents of the downloaded key file to the **~/.ssh/authorized_keys** file.

- To use a custom private key, click **Custom Key**.

  (Optional) In the **Passphrase** field, enter the passphrase created when you generated the private key.

  Next to the **Private Key** field, click the Browse button to upload the private key.

f. (Optional) In the **Fingerprint** field, enter the fingerprint of the remote server.

5. (Optional) Select the check box next to the SMTP Server label to configure Junos Space Network Management Platform to send the report to the email addresses you specify.

   To add Email recipients for reports:

   a. In the **Email Address** field, enter the e-mail address.

   b. Click **Add**.

      You can add multiple e-mail addresses if you want the report to be delivered to multiple e-mail addresses.

6. Click the **Schedule at a later time** check box and specify the date and time to generate the report automatically.

> **NOTE:** If a report generation is already scheduled for later using password mode, in order to use Space Key or Custom Key, you must cancel the existing scheduled task and reschedule it using the authentication mode of your choice.
>
> If a report generation is already scheduled for later using Custom Key and if the key has changed, you must cancel the existing scheduled task and reschedule it using the updated key.

7. Click the **Recurrence** check box and specify the frequency at which to generate the report.

8. Click **Generate**.

   The Generated Report Job Information dialog box appears, displaying the job ID. Click the job ID to view the job details on the Job Management page.

9. Click **OK** to close the Generated Report Job Information dialog box.

   The reports you generated or scheduled are listed on the Generated Reports page. You can view, download, or print the reports.

Release History Table

Release	Description
17.1R1	You can select the authentication mode for saving reports to SCP server from Junos Space Network Management Platform Release 17.1R1 onward.

RELATED DOCUMENTATION

Reports Overview | 768

Creating Report Definitions | 780

Viewing a Report

You view a report when you need to view the details of the report.

To view the details of a report:

1. On the Network Management Platform user interface, select **Reports > Generated Reports**.

The Generated Reports page that appears displays the reports.

2. Select the report you want to view and select the **View Generated Report Details** icon from the Actions bar.

   The View Report dialog box is displayed.

   Table 52 lists the details of the report displayed in the View Report dialog box.

   Table 103: View Report Dialog Box Details

Field or Area	Description	Displayed In
Name	Name of the report	View Generated Report page View Report dialog box
Description	Description of the report	View Generated Report page View Report dialog box
Generated By	Username of the user who generated the report	View Generated Report page View Report dialog box
Generated Time	Time when the report was generated	View Generated Report page View Report dialog box
Report Definition Name	Report definition used to generate the report	View Generated Report page View Report dialog box
Report Format	Formats of report available to view or download: CSV, PDF, and HTML	View Generated Report page View Report dialog box

3. Click **Close** to close the View Report dialog box.

RELATED DOCUMENTATION

Generating Reports | 789

Viewing and Downloading Generated Reports | 794

Deleting Generated Reports | 795

Reports Overview | 768

Viewing and Downloading Generated Reports

You can view and download the reports you generated on the Generated Reports page in the Reports workspace. You can view the name of the report, description of the report, name of the report definition, user who generated the report, time the report was generated, formats in which the report is available, link to view and download the report, and job ID for the report generated.

> **NOTE:** You cannot view or download a report if the report contains a type of report that you do not have access to. The following error message is displayed if you try to view or download such a report: **The selected report contains object categories that you cannot access and hence cannot be viewed/downloaded.** For information about the mapping of report definition categories to the privileges you require, see "Reports Overview" on page 768.

To view and download the reports you generated:

1. On the Junos Space Network Management Platform user interface, select **Reports** > **Generated Reports**.

   The Generated Reports page that appears displays all the reports in the Junos Space Network Management Platform database.

2. Click the **View/Download** link corresponding to the report you want to view or download.

   The Download page is displayed.

3. Select the report formats of the report you want to view or download by clicking the appropriate buttons.

4. (Optional) Save the report to your local computer.

5. Click **Close** to return to the Generated Reports page.

RELATED DOCUMENTATION

Reports Overview | 768

Generating Reports | 789

Deleting Generated Reports

You can delete the reports you generated from the Generated Reports page.

> **NOTE:** You cannot delete a report if the report contains a type of report that you do not have access to. The following error message is displayed if you try to delete such a report: **The selected report contains object categories that you cannot access and hence cannot be deleted.** For information about the mapping of report definition categories to the privileges you require, see "Reports Overview" on page 768.

To delete the reports you generated:

1. On the Junos Space Network Management Platform user interface, select **Reports** > **Generated Reports**.

   The Generated Reports page that appears displays all the reports in the Junos Space Network Management Platform database.

2. Select the check boxes next to the reports you want to delete and click the Delete Generated Report icon on the toolbar.

   The Delete Report window is displayed.

3. Click **Delete**.

   The reports are deleted. You are redirected to the Generated Reports page.

RELATED DOCUMENTATION

Reports Overview | 768

Generating Reports | 789

Viewing Report Statistics

You can view report statistics when you select the Reports workspace. The Report Count by User bar chart presented on the Reports page displays the number of reports created per user. The chart is interactive.

To view report statistics:

1. On the Junos Space Network Management Platform user interface, select **Reports**.

The Reports page is displayed. This page displays the charts related to reports and report definitions.

2. Click a specific label on the Report Count by User chart.

   You are redirected to the Generated Reports page whose contents are filtered based on the label you clicked.

   To save a chart as an image or to print the chart, right-click the chart and select Save or Print respectively.

RELATED DOCUMENTATION

Reports Overview | **768**

Generating Reports | **789**

Deleting Generated Reports | **795**

7

PART

Network Monitoring

Overview | **798**

Managing Nodes | **809**

Searching for Nodes and Assets | **816**

Managing Outages | **823**

Using the Network Monitoring Dashboard | **828**

Managing and Configuring Events | **833**

Managing and Configuring Alarms | **844**

Managing and Configuring Notifications | **865**

Managing Reports and Charts | **873**

Network Monitoring Topology | **884**

Network Monitoring Administration | **901**

CHAPTER 43

Overview

IN THIS CHAPTER

- Network Monitoring Workspace Overview | 799
- Working with the Network Monitoring Home Page | 802

Network Monitoring Workspace Overview

The Network Monitoring workspace enables you to assess the performance of your network, not only at a point in time, but also over a period of time. This feature enables you to determine trending and diverse other things; for example, whether service-level agreements (SLAs) have been violated.

NOTE: Junos Space Release 14.1 and later supports SNMP monitoring of devices using SNMPv1, SNMPv2c, and SNMPv3.

CAUTION: Although additional network monitoring functionality can be accessed by customizing its XML files, editing these files can affect the functionality of the Network Monitoring workspace. We recommend that you do not edit these XML files unless you are directed to do so by Juniper Networks.

To grant a Junos Space user full privileges to access and perform tasks from the Network Monitoring workspace, the user must be assigned the FMPM Manager role. To grant a Junos Space user read-only access to the Network Monitoring workspace, the user must be assigned the FMPM Read Only User role.

The Network Monitoring workspace supports the following three types of users:

- Administrator role: A user assigned the FMPM Manager role and with access to Global domain can view and administer all devices in the Network monitoring workspace, including all devices that exist in other sub-domains.
- Regular user role: A user assigned the FMPM Manager role but without access to global domain can only view and administer devices in their selected domain. This type of user can also acknowledge and clear alarms.
- Read only user role: A user assigned the FMPM Read Only User role (or a customized role with FMPM access capability except admin tab) in Junos Space. This type of user can only view devices in the selected domain, but cannot access the **Network Monitoring > Admin** workspace and cannot acknowledge or clear alarms.

When a remote user (with the FMPM manager role) logs in from the Junos Space user interface, Junos Space authenticates the user from the remote authentication server as follows:

- If the remote authentication is successful, Junos Space uses the user's login credentials to authenticate with the network monitoring server and either creates or updates the network monitoring local user.
- If the remote authentication fails and the user previously existed on the network monitoring server, Junos Space removes the network monitoring local user.

To analyze and aggregate device-level performance data, and to detect device faults, the Network

Monitoring workspace uses a collection of data from managed elements. Performance data is collected automatically if the SNMP settings are set properly for a discovered device. The following performance data is collected:

- *Collection*
  - View historical performance data by using a graphical monitoring tool that allows customization of the parameters to be displayed and the devices to be monitored.
  - Create graphs and charts.
  - Create and export reports in PDF and HTML formats.
  - Define advanced variables that require calculations for historical performance monitoring.
  - Allow raw data to be rolled up into processed data, allowing data to be processed from a more-specific to a less-specific level (for example, data collected at a quarter hourly interval can be rolled into hourly data, hourly data can be rolled into daily data, daily can be rolled into weekly data, and weekly data can be rolled into yearly data).
- *Thresholds*
  - Set thresholds for performance data values—including specifying warning and error levels.
  - Create threshold graphs.
  - Generate threshold-crossing alarms that can be displayed or forwarded.
- *Faults*
  - Receive SNMP traps directly from devices and other enterprise management systems (EMSs).
  - Forward traps to other EMSs.
  - Generate and display events and alarms.
  - Get basic correlation with alarms; for example, clearing alarms and deduplicating alarms.
  - Detect device faults based on data collected from devices.

You can perform the following tasks from the Network Monitoring workspace:

- Node List: List all the devices under monitoring (see “Viewing the Node List” on page 809).
- Search: Search for devices (see “Searching for Nodes or Nodes with Asset Information” on page 816).
- Outages: View unavailable (down) services (see “Viewing and Tracking Outages” on page 823).
- Events: View events (see “Viewing and Managing Events” on page 833).
- Alarms: View alarms (see “Viewing and Managing Alarms” on page 844).
- Notifications: Display notices received by users (see “Viewing, Configuring, and Searching for Notifications” on page 865).
- Assets: Search asset information and assets inventory (see “Working with Node Assets” on page 820).

- Reports: View reports (see “Viewing Reports” on page 876).
- Charts: View charts (see “Viewing Charts” on page 883).
- Topology: View nodes in the network topology and the events and alarms associated with the nodes (see “Working with Topology” on page 887).
- Admin: Perform system administration (see “Configuring Network Monitoring System Settings” on page 901).

The main Network Monitoring landing page is a dashboard, displaying the most important information about your nodes:

- Nodes with outages
- Availability over the last 24 hours
- Notifications (outstanding notices)
- On-call schedule
- Key SNMP customized (KSC) performance reports (if defined and available)

In addition, from this page you can do quick searches on nodes and resource graphs.

NOTE:

- During the Network Monitoring upgrade process, the modified configuration files are automatically merged. However, if the automatic merge fails, you must manually merge the files that could not be merged by following the procedure explained in the “Updating Network Monitoring After Upgrading the Junos Space Network Management Platform” on page 904 topic
- When you upgrade from Release 13.1 or Release 13.3 to Release 14.1, the **linkd-configuration.xml** file is renamed to **linkd-configuration.xml.old.bak**, and the **enlinkd-configuration.xml** file is added.

RELATED DOCUMENTATION

Network Monitoring Reports Overview | **873**

Updating Network Monitoring After Upgrading the Junos Space Network Management Platform | **904**

Working with the Network Monitoring Home Page

IN THIS SECTION

- Viewing Nodes with Pending Problems | 802
- Viewing Nodes with Outages | 803
- Availability Over the Past 24 Hours | 803
- Viewing Outstanding Notifications | 804
- Viewing Resource Graphs | 804
- Viewing KSC Reports | 805
- Searching for Nodes by Using Quick Search | 806

The Network Monitoring home page displays information about nodes with pending problems and outages, service availability information, and notifications. In addition, you can search for resource graphs and key SNMP customized (KSC) reports, and nodes based on different search criteria.

To access the Network Monitoring home page:

1. On the Junos Space Network Management Platform UI, select **Network Monitoring**.

   The Network Monitoring home page appears displaying following information and fields:

   - Nodes with Pending Problems
   - Nodes with Outages
   - Availability over the past 24 hours
   - Notifications
   - Resource Graphs
   - KSC Reports
   - Quick Search

This topic has the following sections:

Viewing Nodes with Pending Problems

The Nodes with Pending Problems table on the Network Monitoring home page displays the nodes that have unacknowledged alarms (if the number of nodes is 16 or lower) or the **All Pending Problems** link.

The color-coding in the table signifies the alarm severity and the time displayed signifies the amount of time that has elapsed since the last event. For detailed information:

- Click the **Nodes with Pending Problems** or **All Pending Problems** link to view the list of alarms for all nodes.

  The Alarms page appears listing the outstanding alarms for the different nodes.

- Click the *Node-Name* link to view information about the node.

  The subsequent page displays information about the node.

- Click the ***Number of*** **alarms** link for a node to view the outstanding alarms for that node.

  The subsequent page lists the outstanding alarms for the node.

Click **Network Monitoring** in the task tree to go to the Network Monitoring home page.

Viewing Nodes with Outages

The Nodes with Outages table on the Network Monitoring home page displays the list of nodes that have outages. A maximum of 12 nodes is displayed in the table; if more than 12 nodes have outages, the ***Number-of*** **more nodes with outages** link is displayed. For detailed information:

- Click the **Nodes with Outages** or ***Number-of*** **more nodes with outages** link to view the outages for all nodes that have outages.

  The Outages page appears, listing the current outages for all the nodes with outages.

- Click the *Node-Name* link to view the information about the node.

  The subsequent page displays information about the node.

Click **Network Monitoring** in the task tree to go to the Network Monitoring home page.

Availability Over the Past 24 Hours

The Availability Over the Past 24 Hours table displays the different service-level management (SLM) categories, which are used to determine the service availability of interfaces and services.

For each category, the name of the category is displayed along with the corresponding outages and the service-level availability (percentage) for the category.

The outages are expressed in the *x* of *y* format, where *x* is the number of managed devices and SNMP agents that have outages at any point and *y* is the total number of managed devices and SNMP agents that can be reached to determine network connectivity (availability); for example 570 of 1200. The outages and availability are color-coded according to the following legend: green (normal), yellow (warning), and red (critical).

For detailed information:

- Click the *Category-Name* link to view the outages and availability information for nodes belonging to that category.

  The category page for the specific category displays the nodes for the specific category and the outages for the nodes and the 24-hour availability.

- Click **Overall Service Availability** to view the outages and availability for all the services monitored by Network Monitoring.

  The subsequent page displays the list of nodes and the outages for the nodes and the 24-hour availability.

Click **Network Monitoring** in the task tree to go to the Network Monitoring home page.

Viewing Outstanding Notifications

The Notification table displays information about your outstanding notices and all outstanding notices.

For detailed information:

- Click the **Notification** link to go to a page where you can run queries on notifications.

  The Notifications page appears. For information about how to run queries on notifications, see "Viewing, Configuring, and Searching for Notifications" on page 865.

- Click the **Check** link corresponding to the **You** field to view the details of the outstanding notices for which you (the logged-in user) were notified.

  The subsequent page displays your outstanding notices.

- Click the **Check** link corresponding to the **All** field to view the details of all outstanding notices.

  The subsequent page displays all outstanding notices.

- The **On Call Schedule** link is currently not supported on Junos Space Platform.

Click **Network Monitoring** in the task tree to go to the Network Monitoring home page.

Viewing Resource Graphs

The Resource Graphs table allows you to view all resource graphs or resource graphs for a specific node; a node might have one more resources associated with it.

- To view all resource graphs, click the **Resource Graph** link.

  The subsequent page t displays the different nodes and you can view standard and custom resource performance reports for different resources.

- To view resource graphs for a specific node:

  1. Enter the full name or a part of the name of the node in the text box.

> **NOTE:** If you enter a string of characters, the search results return a list of nodes that contain the characters in the name. For example, entering **mx** lists all the nodes that contain the characters “mx” within the node name.

2. Click **Search**.

   The list of nodes matching the name that you entered is displayed below the text box.

3. Select the node for which want to view the resource graphs.

   The subsequent page displays the node resources that can be graphed (standard performance graphs).

Click **Network Monitoring** in the task tree to go to the Network Monitoring home page.

Viewing KSC Reports

The KSC Reports table allows you to view all KSC reports or KSC reports for a for a specific resource.

- To view all KSC reports, click the **KSC Reports** link.

  The subsequent page displays the different resources and you can view standard and custom resource performance reports for different resources.

- To view KSC reports for a specific resource:

  1. Enter the full name or a part of the name of the resource in the text box.

     > **NOTE:** If you enter a string of characters, the search results return a list of nodes that contain the characters in the name. For example, entering **mx** lists all the nodes that contain the characters “mx” within the node name.

  2. Click **Search**.

     The list of nodes matching the name that you entered is displayed below the text box.

  3. Select the node for which want to view the resource graphs.

     The subsequent page displays the node resources that can be graphed (standard performance graphs).

Click **Network Monitoring** in the task tree to go to the Network Monitoring home page.

Searching for Nodes by Using Quick Search

You can use the Quick Search feature on the Network Monitoring home page to search for nodes monitored by the Network Monitoring workspace:

- To view all nodes, click the **Search** button corresponding to the **Node ID**, **Node label like**, or **TCP/IP Address like** fields.

  The subsequent page displays the nodes and their interfaces. For more information, see "Viewing the Node List" on page 809.

- To search for a specific node by using the node ID:

  1. Enter the node ID in the **Node ID** field.

  2. Click **Search**.

     - If the node ID that you entered matches the node ID of an existing node, the subsequent page displays the details of the node.
     - If the node ID that you entered does not match the ID of an existing node, the subsequent page displays a message indicating that no nodes match.

  3. Click **Network Monitoring** in the task tree to go to the Network Monitoring home page.

- To search for a specific node using the node label:

  1. Enter the full label or a part of label in the **Node ID** field.

     > **NOTE:** If you enter a part of the label, the search results return a list of nodes that contain the characters that you entered. For example, entering **80** lists all the nodes that contain the characters "80" within the node label.

  2. Click **Search**.

     - If the node label that you entered exactly matches the node label of an existing node, the subsequent page displays the details of the node.
     - If the node label that you entered matches two or more nodes, the subsequent page displays the nodes and their interfaces are displayed. For more information, see "Viewing the Node List" on page 809.
     - If the node label that you entered does not match the ID of an existing node, the subsequent page displays a message indicating that no nodes match is displayed.

  3. Click **Network Monitoring** in the task tree to go to the Network Monitoring home page.

- To search for a specific node by using the node IP address:

  1. Enter the full IP address or a part of IP address in the **TCP Address Like** field.

     > **NOTE:** If you enter a part of the IP address, the search results return a list of nodes that match the IP address that you entered. For example, for IPv4 addresses, entering ***.204.*.*** lists all the nodes that contain “204” in the second octet.
     >
     > If you want to use a partial search for IPv6 addresses, you must enter a backslash (\) character before the colon (:); for example, ***\:204\:*\:***

  2. Click **Search**.
     - If the IP address that you entered is an exact match to the IP address of an existing node, the subsequent page displays the details of the node.
     - If the IP address that you entered matches two or more nodes, the subsequent page displays the nodes. For more information, see “Viewing the Node List” on page 809.
     - If the IP address that you entered does not match the ID of an existing node, the subsequent page displays a message indicating that no nodes match.
  3. Click **Network Monitoring** in the task tree to go to the Network Monitoring home page.

- To view the nodes providing a specific service:

  1. Select the service from the **Providing service** list.
  2. Click **Search**.
     - If the service that you selected is managed on only one node, the subsequent page displays the details of the node.
     - If the service that you selected is managed on two or more nodes, the subsequent page displays the nodes and their interfaces are displayed. For more information, see “Viewing the Node List” on page 809.
     - If the service that you selected is not present on any node, the subsequent page displays a message indicating that no nodes match.
  3. Click **Network Monitoring** in the task tree to go to the Network Monitoring home page.

Click **Network Monitoring** in the task tree to go to the Network Monitoring home page.

RELATED DOCUMENTATION

Viewing the Node List | 809
Viewing and Managing Alarms | 844
Viewing and Tracking Outages | 823
Viewing the Network Monitoring Dashboard | 828

CHAPTER 44

Managing Nodes

IN THIS CHAPTER

- Viewing the Node List | 809
- Managing Surveillance Categories | 811
- Resynchronizing Nodes in Network Monitoring | 813
- Turning SNMP Data Collection Off and On | 814

Viewing the Node List

Junos Space Network Management Platform is monitored by default using the built-in SNMP manager. The Junos Space Network Management Platform node is listed in the node list, and referred to hereafter as the Junos Space Network Management Platform node.

Select **Network Monitoring > Node List**. The Node List page appears. This page displays a list of your nodes and enables you to drill down into each of them.

From the Node List page, you can also access the Resync Nodes subtask (see "Resynchronizing Nodes in Network Monitoring" on page 813).

The Node List page displays a list of all the nodes in your network. You can also display the interfaces for each node. The top level of the Node List page displays only the hostname of each node. Click the hostname of a node to see the following information:

- SNMP Attributes
- Information about the protocols enabled; for example, IS-IS Information
- Availability
- Node Interfaces—IP Interfaces and, if applicable, physical Interfaces

> **NOTE:** IPv6 MIBs are supported only on Junos OS Release 13.2 and later. Therefore, if the version of Junos OS running on a device is Release 13.1 or earlier, the following are applicable:
>
> - The ifIndex parameter is not displayed for IPv6 interfaces.
> - Only the IPv6 address used by Junos Space Platform to manage the device is displayed; other interfaces that are configured with IPv6 addresses are not displayed.
> - When the device is discovered by using the IPv4 address, the IPv6 interfaces are not displayed.

- General—Status of the node and detailed information about the node.

  Click the **View Node Link Detailed Info** hyperlink to view the following information discovered by the EnhancedLinkd daemon:

  - Link Layer Discovery Protocol (LLDP) remote table links
  - IS-IS adjacent table links
  - OSPF neighbor links

  > **NOTE:** If the EnhancedLinkd daemon does not discover links for a protocol, no information is displayed for that protocol.

- Surveillance Category Memberships
- Notifications
- Recent Events
- Recent Outages

Each of these items has links that enable you to drill deeper into the corresponding aspect of the node's performance.

For each node, you can also view events, alarms, outages and asset information; and rescan, access the admin options, and schedule outages.

RELATED DOCUMENTATION

Network Monitoring Workspace Overview | 799

Viewing Managed Devices | 194

Resynchronizing Nodes in Network Monitoring | 813

Viewing and Managing Alarms | 844
Viewing, Configuring, and Searching for Notifications | 865
Working with Node Assets | 820

Managing Surveillance Categories

IN THIS SECTION

- Modifying Surveillance Categories | 811
- Deleting Surveillance Categories | 811
- Adding Surveillance Categories | 812

You can specify the devices for which SNMP data collection is controlled in different surveillance categories. Surveillance categories determine whether the data for the device is collected for performance management monitoring. You can modify, delete, and add surveillance categories.

Modifying Surveillance Categories

To modify a surveillance category:

1. Select **Network Monitoring > Admin > Manage Surveillance Categories**.
2. Click the icon in the Edit column in the same row as the category.

   The Edit Surveillance Category page appears.
3. To add devices to the surveillance category, select the device from the Available nodes list and click **Add**.
4. To remove devices from the surveillance category, select the device from the Nodes on category list and click **Remove**.

Deleting Surveillance Categories

To remove a surveillance category, click the icon in the Delete column in the same row as the category.

Adding Surveillance Categories

To add a surveillance category:

1. Select **Network Monitoring > Admin > Manage Surveillance Categories**.

2. Enter the name in the box and click **Add New Category**.

   The name appears on the Surveillance Categories page.

3. Click the name in the Category column, and click **Edit category** on the Surveillance Category page.

4. To add devices to the surveillance category, select the device from the Available nodes list and click **Add**.

5. To remove devices from the surveillance category, select the device from the Nodes on category list and click **Remove**.

RELATED DOCUMENTATION

Turning SNMP Data Collection Off and On | 814

Network Monitoring Workspace Overview | 799

Resynchronizing Nodes in Network Monitoring

You should resynchronize your nodes when the contents of the Node List page in the Network Monitoring workspace do not correspond with the device listed on the Device Management page in the Devices workspace.

In addition, you must resynchronize nodes when you want to update the trap target settings on the devices so that the devices can send traps to Network Monitoring. For more information, see the explanation for the **Add SNMP configuration to device for fault monitoring** and **Disable network monitoring for all devices** fields in the "Modifying Junos Space Network Management Platform Settings" on page 1346 topic.

When you trigger node resynchronization, Junos Space Platform synchronizes the devices and their details with Network Monitoring and pushes the SNMP trap target configuration to the devices so that the devices can send SNMP trap targets to Network Monitoring.

The following are applicable when you resynchronize nodes:

- If you are in a specific domain when you resynchronize nodes, only the devices that are part of that domain are resynchronized with Network Monitoring.
- The Resync Nodes job summary displays the information related to synchronization in Network Monitoring and the status of the trap target update.
- When you resynchronize nodes, Junos Space Platform does not set the SNMP trap target on logical systems (LSYS), unmanaged devices, modeled devices, and devices that are down.
- If you attempt to resynchronize nodes in a particular domain when a Resync Nodes job is already running in that domain, Junos Space Platform provides a notification that you cannot run another Resync Nodes job until the previous one is completed.

To resynchronize your nodes:

1. In the Junos Space Network Management Platform UI, select **Network Monitoring** > **Node List** > **Resync Nodes**.

   You are taken to the Resync Nodes page, where a confirmation dialog box is displayed.

2. Click **Confirm**.

   The Resync Nodes Job Information dialog box appears.

3. (Optional) To view details of the resynchronization job, click the hyperlinked job ID displayed in the dialog box.

   You are taken to the Job Management page where you can view the summary information about the Resync Nodes job. Double-click the job to view detailed information about the job.

4. Click **OK** in the Resync Nodes Job Information dialog box.

You are taken to the Node List page. After the Resync Nodes job is completed successfully, the devices in Junos Space Platform are synchronized with Network Monitoring and, if applicable, the device trap targets are updated. The resynchronized nodes are displayed on the Node List page.

> **NOTE:** The time taken for the resynchronization of devices from Junos Space Platform to Network Monitoring depends on the number of devices being synchronized.

RELATED DOCUMENTATION

- Network Monitoring Workspace Overview | 799
- Viewing the Node List | 809
- Turning SNMP Data Collection Off and On | 814
- Viewing Managed Devices | 194

Turning SNMP Data Collection Off and On

Network performance can be adversely affected by the amount of traffic generated by SNMP data collection. For this reason, SNMP service in Junos Space Network Management Platform is not started by default.

Junos Space Network Management Platform Network Monitoring is always turned on for all devices by default. The ability to turn on data collection is controlled by the Monitor_SNMP surveillance category. However, turning on data collection increases the amount of SNMP traffic. If the surveillance category is removed from a device, data collection is turned off.

To turn SNMP data collection off or on for a device:

1. In the Network Monitoring workspace, display the Node List page and click the node name.

   The resulting page displays detailed information about the device.

   For example, you can select **Network Monitoring > Node List** or you can select **Network Monitoring > Search** and click **All nodes** in the Search for Nodes section of the Search page to display the Node List page.

2. In the Surveillance Category Memberships title bar, click **Edit**.

   The Edit surveillance categories on *node name* page appears.

3. Select the **Monitor_SNMP** category from the Categories On Node list on the right.

   If this category is *not* in the list on the right, then SNMP data collection is already turned off.

4. Click **Remove** between the two lists.

   The removed category appears in the list of Available Categories on the left.

To turn on data collection for selected devices, reverse the process described here.

> **NOTE:** The Network Monitoring functionality performs SNMP data collection by default only on primary interfaces. If you want to change this, instead of manually selecting the interfaces to be monitored from the GUI, you can set data collection for all interfaces by default by modifying the SNMP collection to set the SNMP Storage Flag to **all** (see "Managing SNMP Collections" on page 924). For information on the procedure to select other interfaces and the distinction between primary and secondary interfaces, see "Configuring SNMP Data Collection per Interface" on page 913.

RELATED DOCUMENTATION

Viewing the Node List | **809**

Searching for Nodes or Nodes with Asset Information | **816**

Viewing the Network Monitoring Dashboard | **828**

CHAPTER 45

Searching for Nodes and Assets

IN THIS CHAPTER

- Searching for Nodes or Nodes with Asset Information | 816
- Working with Node Assets | 820

Searching for Nodes or Nodes with Asset Information

IN THIS SECTION

- Searching for Nodes | 816
- Searching for Nodes with Asset Information | 818

You can search for nodes or for nodes with asset information in the Network Monitoring workspace by using different search criteria.

To access the Network Monitoring Search page:

1. On the Junos Space Network Management Platform UI, select **Network Monitoring** > **Search**.

   The Search page, which is divided into the following sections, appears:

   - Search for Nodes—You can search for nodes by using various fields or view all nodes and interfaces.
   - Search Asset Information—You can search for node asset information using various criteria or view all nodes with asset information.
   - Search Options—This table provides tips about the various search fields on the Search page.

This topic has the following sections:

Searching for Nodes

You can search for nodes by using different parameters, or view all nodes or all nodes and their interfaces:

- To search for nodes:

1. You can search for nodes by using one of the following parameters:
   - To search for a node using the node name, enter the full name or a part of the name in the (non-case-sensitive) **Name containing** field.

     NOTE:
     - If you enter a part of the name, the search results return a list of nodes that contain the characters that you entered. For example, entering **MX** lists all the nodes that contain the characters "MX" within the node name.
     - Use _ (underscore) to represent a single character wildcard and % to represent a multicharacter wildcard.

   - To search using the node or interface IP address, enter the full IP address or a part of IP address in the **TCP Address Like** field.

     NOTE:
     - If you enter a part of the IP address, the search results return a list of nodes that match the IP address that you entered. For example, entering ***.204.*.*** lists all the nodes that contain 204 in the second octet.
     - You can also use a combination of the following:
       - A single * (asterisk) as a wildcard for an octet
       - A hyphen to specify an octet range
       - A comma to demarcate two or more numbers within an octet

       For example, 192.168.*.*, 192.*.0,1,2.1-10, and so on
     - For IPv6 addresses, you must enter the full IP address and not the shortened form; however, * (asterisk) is supported as a wildcard.

   - To search for nodes based on the interface alias, name, or description:

     a. Select the interface parameter on which to search for the node from the list:
        - Select **ifAlias** to search using the interface alias.
        - Select **ifName** to search using the interface name.
        - Select **ifDescr** to search using the interface description.

     b. Select whether you want to search for interfaces that contain the interface parameter (**contains**) or are an exact match (**equals**) to the interface parameter.

c. Enter the text that you want to search for in the text box.

> **NOTE:** The wildcard characters are the same as the ones used in the **Name containing** field.

- To find nodes providing a specific service, select the service from the **Providing service** field.
- To search for nodes based on the interface MAC address, enter the full or partial MAC address (non-case-sensitive) in the **MAC Address like** field.

> **NOTE:**
> - The wildcard characters are the same as the ones used in the **Name containing** field.
> - The octet separators in the MAC address (hyphen or colon) are optional.

- You can search for nodes based on whether they are devices managed by Junos Space (**space**) or nodes in the Junos Space fabric (**fabric** using the **Foreign Source name like** field.

2. Click the **Search** button corresponding to the search parameter that you specified. For example, if you searched for nodes by using the **TCP/IP Address like** field, click the **Search** button corresponding to that field.
   - If the search parameter that you entered exactly matches an existing node, the subsequent page displays the details of the node.
   - If the search parameter that you entered matches two or more nodes, the subsequent page displays the nodes and their interfaces.
   - If the search parameter that you entered does not match any node, the subsequent page displays a message indicating that no nodes match.

- To view all nodes, click the **All nodes** link.

  The subsequent page displays all nodes.
- To view all nodes and their interfaces, click the **All nodes and their interfaces** link.

  The subsequent page displays the nodes and their interfaces.

Searching for Nodes with Asset Information

You can search for nodes based on the node asset information or view all nodes that contain asset information:

- To search for nodes based on asset information:

1. You can search for nodes by using one of the following parameters:
   - To search for a nodes belonging to an asset category, select the category from the **Category** list.
   - To search for nodes based on a specific asset information field:
     a. Select the asset information field that you want to search for using the **Field** list.
     b. Enter the text that you want to search for (non-case-sensitive) in the **Containing text** field.

     NOTE:
     - If you enter a part of the asset information field, the search results return a list of nodes that contain the characters that you entered. For example, selecting **City** and entering **York** lists all the nodes with asset information that contain the characters York in the **City** field.
     - Use _ (underscore) to represent a single character wildcard and % to represent a multicharacter wildcard.

2. Click the **Search** button corresponding to the search parameter that you specified. For example, if you searched for nodes by using the **Category** field, click the **Search** button corresponding to that field.
   - If the search parameter that you entered matches one or more nodes, the subsequent page displays the asset link and the node link for each node.
   - If the search parameter that you entered does not match any node, the subsequent page displays a message indicating that no nodes match.

- To view all nodes that have asset information associated with them, click the **All nodes with asset info** link.

  The subsequent page displays the asset link and the node link for each node with asset information.

RELATED DOCUMENTATION

Network Monitoring Workspace Overview | 799

Viewing the Node List | 809

Viewing Managed Devices | 194

Working with Node Assets | 820

Working with Node Assets

IN THIS SECTION

- Searching for and Viewing Nodes with Asset Information | 820
- Viewing and Modifying Node Asset Information | 821

On the Network Monitoring Assets page, you can view the node asset information, search for assets based on asset category, view all nodes with asset information, and modify the asset information for a node. Asset information includes the information about devices, such as device configuration category information, device identification information, device location, and so on.

To access the Assets page:

1. On the Junos Space Network Management Platform UI, select **Network Monitoring** > **Assets**.

   The Assets page, which is divided into the following sections, appears:

   - Search Asset Information—You can search for assets based on asset categories or view all nodes with asset information.
   - Assets with Asset Numbers—This table displays the nodes that contain the information about asset numbers. Click the node name link to view the details of the asset.
   - Assets Inventory—This table provides information about how to use assets in Network Monitoring.

This topic has the following sections:

Searching for and Viewing Nodes with Asset Information

You can search for nodes based on asset categories or view all nodes that have asset information:

- To search for nodes based on asset category:
  1. Select the category from the **Assets in category** list.
  2. Click the **Search** button.
     - If there are nodes that belong to the specified asset category, the subsequent page displays the asset link and the node link for each node:
       - Click the *Asset Link* link to view or modify the asset information for a node.

         In the subsequent page, you can view or modify the asset information. For details, refer to "Viewing and Modifying Node Asset Information" on page 821

- Click the *Node Link* link to view information about the node.

  The subsequent page displays information about the node.

- If the asset category that you specified does not match any node, the subsequent page displays a message indicating that no nodes have been found.

- To view all nodes that have asset information, click the **All nodes with asset info** link.

  The subsequent page displays the asset link and the node link for each node with asset information.

  - Click the *Asset Link* link to view or modify the asset information for a node.

    In the subsequent page, you can view or modify the asset information. For details, refer to "Viewing and Modifying Node Asset Information" on page 821

  - Click the *Node Link* link to view information about the node.

    The subsequent page displays information about the node.

Viewing and Modifying Node Asset Information

On the asset modification page, you can view and modify asset information for a node. The asset information for the node (**Asset Info of Node *Node-ID***) is displayed in the following tables:

- **SNMP Info**—Displays system information for the node obtained by using the SNMP agent

  > **NOTE:** You cannot modify the fields in this table

- **Configuration Categories**—Displays different categories that you can use to group devices
- **Identification**—Displays identifying information for the node such as model number, asset number, and so on
- **Location**—Displays location information for the node
- **Vendor**—Displays information about the vendor providing service for the node
- **Authentication**—Displays authentication information for SSH, Telnet, and remote shell (rsh)
- **Hardware**—Displays hardware information for the node
- **VMWare**—Displays information related to VMware-based devices
- **Comments**—Displays comments

To modify the asset information:

1. Click the field that you want to modify and make the changes.

NOTE: Network Monitoring performs validation checks on some of the fields. Refer to the legend at the bottom of this page for an explanation of the color-coding.

2. After you have modified the fields:
   - Click **Save** to save the changes.

     The modifications are saved and displayed on the same page.
   - Click **Reset** to discard the changes and revert to the last-saved information in the fields.

RELATED DOCUMENTATION

- Network Monitoring Workspace Overview | **799**
- Viewing the Node List | **809**
- Viewing Managed Devices | **194**
- Resynchronizing Nodes in Network Monitoring | **813**
- Searching for Nodes or Nodes with Asset Information | **816**

CHAPTER 46

Managing Outages

IN THIS CHAPTER

- Viewing and Tracking Outages | 823
- Configuring Scheduled Outages | 826

Viewing and Tracking Outages

IN THIS SECTION

- Viewing Details about an Outage | 824
- Viewing the List of Outages | 825

When you provision services on nodes, Network Monitoring tracks these services by polling them and creating outages if services do not respond to polls. Using the Outages page, you can view the outage information for a single outage, view current outages, or view both current and resolved outages.

To view a list of outages and information about outages:

1. On the Junos Space Network Management Platform UI, select **Network Monitoring** > **Outages**.

   The Outages page appears.

2. (Optional) To view detailed information about an outage:

   a. In the **Outage ID** text box, enter the ID of the outage.

   b. Click **Get Details** or press Enter.

   - If the outage ID that you entered matches an existing outage, the subsequent page displays information about the outage. For more information, refer to "Viewing Details about an Outage" on page 824.

- If the outage ID that you entered does not match an existing outage, the subsequent page displays a message to this effect. You can reenter an outage ID or view a list of the current outages.

3. (Optional) To view the list of the current outages, click the **Current Outages** link.

   The Outages (List) page appears displaying the list of current outages in a table. For more information, refer to "Viewing the List of Outages" on page 825.

4. (Optional) To view the list of all (resolved and current) outages, click the **All Outages** link.

   The Outages (List) page appears displaying the list of all outages in a table. For more information, refer to "Viewing the List of Outages" on page 825.

This topic has the following sections:

Viewing Details about an Outage

In the **Outage: *outage-id*** table, the following information, as shown in Table 104, about an outage is displayed.

Table 104: Details of a Service Outage

Field	Description
Node	Name of the node on which the outage occurred You can click the ***Node*** link to view details about the node.
Interface	Interface on which the outage occurred You can click the ***Interface*** link to view details about the interface.
Service	Service that was affected by the outage You can click the ***Service*** link to view details about the service.
Lost Service Time	Date and time when the service outage occurred
Regained Service	Date and time when the service was restored
Lost Service Event	ID of the event that was generated when the service outage occurred You can click the ***Lost Service Event*** link to view details of the event.
Regained Service Event	ID of the event that was generated when the service was restored You can click the ***Regained Service Event*** link to view details of the event.

Viewing the List of Outages

On the Outages (List) page, the list of current outages is displayed in a table, as shown in Table 105. Depending on how you accessed this page, the page might display the current outages or both the current and resolved outages.

You can view outages based on the type of outage (current, resolved, or both), and filter and sort the list of outages displayed based on various criteria:

1. (Optional) To view outages of a specific type, from the **Outage type** list, select whether you want to view current outages, resolved outages, or both current and resolved outages.

   The outages are displayed based on your selection.

2. (Optional) To sort the outages displayed:

   - In descending order, click the column name in the table once.
   - In ascending order, click the column name in the table twice.

   The outages are sorted based on the column that you clicked.

3. (Optional) To filter outages based on different constraints:

   - Based on foreign source, node, or interface, click the plus (+) icon to view outages only for the corresponding parameter or click the minus (–) icon to exclude outages for the corresponding parameter.
   - Based on the date and time when the service outage occurred, click the back arrow icon to view outages that occurred after the corresponding date and time or click the forward arrow icon to view outages that began before the corresponding date and time.
   - Based on the date and time when the service was restored, click the back arrow icon to view outages that were resolved after the corresponding date and time or click the forward arrow icon to view outages that were resolved before the corresponding date and time.

   The outages in the table are displayed based on the constraints that you applied.

   NOTE: When you apply one or more constraints, the applied constraints are displayed in the **Search constraints** field. You can click the minus (–) icon to remove a constraint.

NOTE: If the list of outages displayed runs across multiple pages, you can use the navigation links in the **Results** field near the top of the page to view the outages.

Table 105: Fields on the Outages (List) Page

Field	Description
ID	Outage ID You can click the ***ID*** link to view details about the outage.
Foreign Source	External name of the node on which the outage occurred
Node	Name of the node on which the outage occurred You can click the ***Node*** link to view details about the node.
Interface	Interface on which the outage occurred You can click the ***Interface*** link to view details about the interface.
Service	Service that was affected because of the outage You can click the ***Interface*** link to view details about the interface.
Down	Date and time when the service outage occurred
Up	Date and time when the service was restored **NOTE:** This field displays **DOWN** if the service is not yet restored.

RELATED DOCUMENTATION

- Viewing and Managing Alarms | 844
- Viewing, Configuring, and Searching for Notifications | 865
- Viewing and Managing Events | 833
- Searching for Nodes or Nodes with Asset Information | 816
- Viewing the Node List | 809

Configuring Scheduled Outages

You can configure scheduled outages to suspend notifications, polling, thresholding, and data collection (or any combination of these) for any interface or node for any length of time.

To create a scheduled outage:

1. Select **Network Monitoring > Admin > Scheduled Outages**.

2. Specify a name for the scheduled outage.

3. Click **Add new outage** to create the scheduled outage.

4. Build the rule that determines which nodes are subject to this critical path.

5. Specify appropriate values for the following fields:
   - Node Labels—From the list, select the node labels to add.
   - Interfaces—From the list, select the interfaces to add.
   - Outage type—From the list, select daily, weekly, monthly, or (time) specific.
   - Time—Specify one or more days and times for the outage.
6. Specify that the outage applies to one or more of the following categories:
   - Notifications
   - Status polling
   - Threshold checking
   - Data collection

CHAPTER 47

Using the Network Monitoring Dashboard

IN THIS CHAPTER

- Viewing the Network Monitoring Dashboard | 828

Viewing the Network Monitoring Dashboard

IN THIS SECTION

- Using the Dashboard Surveillance View | 829

The Network Monitoring Dashboard page displays information about nodes based on the surveillance view configured for the user (in the **/opt/opennms/etc/surveillance-views.xml** file).

To access the Network Monitoring Dashboard page:

1. Select **Network Monitoring** > **Dashboard**.

   The Dashboard page, which has five sections or tables (also known as dashlets), appears:

   > **NOTE:** If the Dashboard does not display information about all your nodes, you should resynchronize your nodes in Network Monitoring. For more information, see "Resynchronizing Nodes in Network Monitoring" on page 813.

   - Surveillance View—Displays surveillance categories in a table as determined by the configuration in the **/opt/opennms/etc/surveillance-views.xml** file
   - Alarms—Displays alarms on the nodes
   - Notifications—Displays notifications on the nodes.
   - Node Status—Displays status of the nodes.
   - Resource Graphs—Displays the first resource graph for the first node

Using the Dashboard Surveillance View

The **Surveillance View:*view-name*** dashlet determines what content is displayed on the other dashlets on the Dashboard page. By default, information about all the nodes that are part of the surveillance view (**Show all nodes** option) is displayed on the Dashboard page.

> **NOTE:**
> - The rows and columns (surveillance categories) displayed in the **Surveillance View:*view-name*** table (dashlet) are determined by the configuration in the **/opt/opennms/etc/surveillance-views.xml** file.
> - The color-coding in the cells in the table is based on the severity of the event.

You can control the display of information in the other dashlets on this page by one of the following tasks:

- Click the first column of a row or column to restrict the information displayed in the rest of the dashlets to the nodes that belong to that surveillance category. The row or column that you clicked is highlighted.
- Click a cell in the table (other than the one in the first row or column) to restrict the information displayed in the rest of the dashlets to the nodes that belong to the surveillance categories defined by the row and column. The cell that you clicked is highlighted.

Depending on the selection in the **Surveillance View:*view-name*** dashlet, the **Alarms**, **Notifications**, **Node Status**, and **Resource Graphs** display information about the nodes that match the surveillance categories.

- The **Alarms** dashlet (table) displays the outstanding alarms for the nodes selected in the **Surveillance View** dashlet. In the header of the table, the total number of alarms and the current count of the alarms (for example, 6 to 10 of 34) are displayed. The information displayed about each alarm is shown in Table 106. You can click **<<** to view the preceding set of alarms or click **>>** to view the next set of alarms.
- The **Notifications** dashlet (table) displays the notifications for the nodes selected in the **Surveillance View** dashlet. In the header of the table, the total number of notifications and the current count of the notifications (for example, 1 to 5 of 12) are displayed. The information displayed about each notification is shown in Table 107. You can click **<<** to view the preceding set of notifications or click **>>** to view the next set of notifications.
- The **Node Status** dashlet (table) displays the status of the nodes selected in the **Surveillance View** dashlet; a node is displayed in this table only if a service on the node is down. In the header of the table, the total number of nodes and the current count of the nodes are displayed. The information displayed about each node is shown in Table 108. You can click **<<** to view the preceding set of nodes or click **>>** to view the next set of nodes.
- The **Resource Graphs** dashlet (table) enables you to view the resource graphs of the nodes selected in the **Surveillance View** dashlet. The fields displayed in this dashlet is shown in Table 109. You can click **<<** to view the preceding resource graph or click **>>** to view the next resource graphs. The default period over which the graphs are plotted is one week.

Table 106: Fields Displayed in the Alarms Dashlet (Table)

Field	Description
Node	Name of the node on which the alarm occurred You can click the node name link to view detailed information about the node.
Log Msg	Log message associated with the alarm Mouse over this cell to view the description associated with the alarm.
Count	Number of times that the alarm has occurred
First Time	Date and time when the alarm was first triggered
Last Time	Date and time when the alarm was last triggered

Table 107: Fields Displayed in the Notifications Dashlet (Table)

Column Heading	Content
Node	Name of the node on for which the notification was created You can click the node name link to view detailed information about the node.

Table 107: Fields Displayed in the Notifications Dashlet (Table) *(continued)*

Column Heading	Content
Service	Name of the service for which the notification was sent
Message	Contents of the notification
Sent Time	Date and time when the notification was sent
Responder	User who received the notification
Response Time	Date and time when the response was sent

Table 108: Fields Displayed in the Node Status Dashlet (Table)

Field	Description
Node	Name of the node You can click the node name link to view detailed information about the node.
Current Outages	Number of service outages on the node expressed in the *x* of *y* format, where *x* is the number of current service outages and *y* is the total number of services on the node; for example 1 of 6.
24 Hour Availability	Percentage of time in the last 24 hours when the node actually was up, expressed as a percentage; for example, 93.391%

Table 109: Fields Displayed in the Resource Graphs Dashlet (Table)

Field	Description
Node *name*	Name of the nodes
Information options available for the selected node (at the node or interface level)	Varies, depending on the category of node selected, for example: For routers: SNMP Node Data, SNMP Interface Data, Response Time, BGP Peer, OSPF Area Info For switches: Response Time
Filename of the resource graph selected from the list (SNMP OID-based performance data)	Below the filename, the selected graph is displayed

RELATED DOCUMENTATION

Turning SNMP Data Collection Off and On | 814

Resynchronizing Nodes in Network Monitoring | 813

Working with the Network Monitoring Home Page | 802

CHAPTER 48

Managing and Configuring Events

IN THIS CHAPTER

- Viewing and Managing Events | 833
- Selecting and Sending an Event to the Network Management System | 840
- Managing Events Configuration Files | 841

Viewing and Managing Events

IN THIS SECTION

- Viewing the Details of an Event | 834
- Searching for Events (Advanced Event Search) | 835
- Viewing, Searching for, Sorting, and Filtering Events | 837

In the Network Monitoring workspace, events refer to any changes detected in the network. Events can be generated internally by Network Monitoring or through external SNMP traps.

You can set various parameters, such as an event description, log message, severity, and so on, when an event is generated by using the **eventconf.xml** file. In addition, you can specify that event parameters are sent to an external script.

To search for and view information about events:

1. On the Junos Space Network Management Platform UI, select **Network Monitoring** > **Events**.

   The Events page appears.

2. (Optional) To view detailed information about an event:

   a. In the **Event ID** text box (in the **Event Queries** section), enter the ID of the event.

b. Click **Get Details** or press Enter.

- If the event ID that you entered matches an existing event, the subsequent page displays information about the event. For more information, see "Viewing the Details of an Event" on page 834.
- If the event ID that you entered does not match an existing event, the subsequent page displays where a message to this effect.

3. (Optional) To view the list of all events, click the **All events** link (in the **Event Queries** section).

   The Events (List) page appears and the list of events is displayed in a table. For more information, see "Viewing, Searching for, Sorting, and Filtering Events" on page 837

4. (Optional) To search for events by specifying one or more search criteria, click the **Advanced Search** link (in the **Event Queries** section).

   The **Advanced Event Search** page appears. For more information, see "Searching for Events (Advanced Event Search)" on page 835.

5. (Optional) If event filter favorites were previously created, you can perform the following tasks in the **Event Filter Favorites** section:

   NOTE: You can view and delete only the event filters that you created.

   - View the constraints that are part of a filter by mousing over the information icon corresponding to a filter.

     The constraints are displayed in a pop-up window.

   - View the events that match a filter by clicking the filter name link.

     The Events (List) page appears and the list of events is displayed in a table. For more information, see "Viewing, Searching for, Sorting, and Filtering Events" on page 837.

   - Delete an event filter favorite by clicking the X link corresponding to the filter.

     The favorite is deleted and a message indicating that the favorite is deleted is displayed.

This topic has the following sections:

Viewing the Details of an Event

On the **Event *event-ID*** page, the information about an event, as shown in Table 110, is displayed.

Table 110: Information Displayed About an Event

Field	Description
Severity	Severity of the event: • **Critical**—Numerous devices are affected; fixing the problem is essential. • **Major**—The device is completely down or in danger of going down; immediate attention is required. • **Minor**—Part of a device (service, interface, power supply, and so forth) has stopped; attention is required. • **Warning**—The event might require action; should possibly be logged. • **Indeterminate**—No severity is associated with the event. • **Normal**—This is an informational message; no action is required. • **Cleared**—This indicates that a prior error condition has been corrected and the service is restored.
Node	Name of the node on which the event occurred You can click the ***Node*** link to view details about the node.
Time	Date and time when the event occurred
Interface	Interface on which the event occurred You can click the ***Interface*** link to view details about the interface.
Service	Service that was affected by the event You can click the ***Service*** link to view details about the service.
UEI	Unique event identifier (UEI) associated with the event Each event in Network Monitoring, including those generated by traps, is assigned a UEI.
Log Message	Message that was logged for the event
Description	Detailed description of the event
Operator Instructions	Instructions for the operator of the node on which the event occurred

Searching for Events (Advanced Event Search)

On the Advanced Event Search page, you can search for events based on one or more fields.

To search for events:

1. (Optional) In the **Event Text Contains** field, enter the text (partial or full) that you want to search for.

   The text that you entered is matched against the **Description** fields.

2. (Optional) In the **TCP/IP Address Like** field, enter the interface IP address in the *.*.*.* format for IPv4 addresses and *:*:*:*:*:*:*:* for IPv6 addresses.

3. (Optional) In the **Node Label Contains** field, enter the name of the node (partial or full).

4. (Optional) Specify the severity of the event using the **Severity** list.

5. (Optional) In the **Exact Event UEI** field, specify the UEI for the event.

   NOTE: You must specify the full UEI if you want to search using this field; partial matches and wildcards are not allowed.

6. (Optional) Select the service that was *affected* by the event using the **Service** list.

7. (Optional) To search for events after a specified date and time, specify the date and time in the **Events After** field.

   NOTE: If you want to search for events within a certain date and time range, you must specify both the **Events After** and **Events Before** fields.

8. (Optional) To search for events before a specified date and time, specify the date and time in the **Events Before** field.

9. (Optional) Specify a sorting order for the search results using the **Sort By** list.

   By default, search results are sorted in descending order of event ID.

10. (Optional) Specify the number of events to display per page using the **Number of Events Per Page** list.

11. Click Search or press Enter when your cursor is inside one of the text boxes.

    The Events (List) page appears and displays the events that match your search parameters. For more information, see "Viewing, Searching for, Sorting, and Filtering Events" on page 837

Viewing, Searching for, Sorting, and Filtering Events

By default, the Events (List) page displays the list of outstanding events in a table. However, depending on whether you used Advanced Search or applied a favorite filter, the list of events displayed might be different. For each event, the information shown in Table 111 is displayed.

You can filter and sort the list of events displayed based on various criteria:

1. (Optional) To apply an existing favorite event filter, select the name of the filter from the **Filter Name** list.

   The events are displayed based on the filter that you applied.

2. (Optional) If you applied a favorite event filter, you can remove it by clicking the **Remove Filter** button.

   All outstanding events are displayed on the Events (List) page.

3. (Optional) To search for events:

   > **NOTE:** You must specify one of the search criteria.

   a. Enter the text (non-case-sensitive) in the **Event Text** field to search for events based on the text in the event log message and description.

   b. From the **Time** list, select the period for which you want to view the events.

   c. Click **Search**.

      The outstanding events that match the search criteria are displayed. The search criteria is displayed in the **Search constraints** field.

4. (Optional) To view a specific number of events per page, select the required number from the list next to the **Results** field.

   By default, the number of events listed on the View Events page is 20. You can select the number of events you want to view per page from the **Show** list. You can choose to view 10, 20, 50, 100, 250, 500, or 1000 events.

   > **NOTE:** The number of events selected is set as user preference and the selected number of events are listed beginning from the next login.

5. (Optional) To sort the events displayed:

- In descending order, click the column name link in the table once.
- In ascending order, click the column name link in the table twice.

The events are sorted based on the column that you clicked.

6. (Optional) To filter events based on different constraints:
   - Based on severity, node, interface, or service, click the plus (+) icon to view events only for the corresponding parameter or click the minus (–) icon to exclude events for the corresponding parameter.
   - Based on the date and time when the event occurred, click the back arrow icon to view events that occurred after the corresponding date and time or click the forward arrow icon to view events that began before the corresponding date and time.

   The events in the table are displayed based on the constraints that you applied. In addition, the constraints that you applied are displayed in the **Search constraints** field.

7. (Optional) You can remove existing search constraints by clicking the minus (–) icon corresponding to a constraint in the **Search Constraints** field.

   NOTE: The **Event(s) outstanding** constraint is applied by default and cannot be removed. You can toggle this constraint with the **Event(s) acknowledged** constraint, which displays the list of acknowledged events, by clicking the minus (–) icon.

8. (Optional) To save a filter as a favorite:

   NOTE: You can save a filter as a favorite only if the filter contains search constraints other than **Event(s) outstanding** or **Event(s) acknowledged**.

   a. Click the **Save Filter** button in the **Search Constraints** field.

      A window is displayed instructing you to enter the name of the favorite filter.

   b. Enter a unique name (up to 30 alphanumeric characters except %, &, or #) for the filter in the text box.

   c. Click **OK**.
      - If an existing favorite filter has the same name, a warning message is displayed on the Events (List) page. You must re-enter a unique name to save the filter.

- If the filter name that you specified is unique, the filter is saved and the Events (List) page appears. The **Filter Names** list displays the name of the filter.

> **NOTE:** Previously saved event filter favorites are accessible from the **Event Filter Favorites** section of the Events page.

9. (Optional) To view all outstanding events, click the **View all events** link at the top of the page.

   The outstanding events are displayed on the Events (List) page.

10. (Optional) To search for events based on multiple criteria, click the **Advanced Search** link at the top of the page.

    The **Advanced Event Search** page appears. For more information, see "Searching for Events (Advanced Event Search)" on page 835

11. (Optional) To view the event severity levels, their color-coding, and explanation, click the **Severity Legend** link at the top of the page.

    The severity levels are displayed in a window. Click the Close (x) button to close the window.

> **NOTE:** If the list of events displayed runs across multiple pages, you can use the navigation links in the **Results** field near the top of the page to view the events.

Table 111: Information Displayed on the Events (List) Page

Field	Description
ID	Event ID You can click the *ID* link to go to the Event Details page.
Severity	Severity of the event Refer to Table 110 for a list of the different severity levels.
Time	Date and time when the event occurred
Node	Name of the node on which the event occurred You can click the ***Node*** link to view details about the node.

Table 111: Information Displayed on the Events (List) Page *(continued)*

Field	Description
Interface	Interface on which the event occurred You can click the ***Interface*** link to view details about the interface.
Service	Service that was affected by the event You can click the ***Service*** link to view details about the service.
None	UEI associated with the event **NOTE:** You can edit the notifications for an event by clicking the **Edit notifications for an event** link. For more information, see "Configuring Event Notifications, Path Outages, and Destination Paths" on page 867.
None	Partial description of the event
None	Message that was logged for the event

RELATED DOCUMENTATION

Viewing the Node List | 809

Searching for Nodes or Nodes with Asset Information | 816

Viewing and Managing Alarms | 844

Selecting and Sending an Event to the Network Management System

To select and send an event:

1. Select **Network Monitoring > Admin > Send Event**.

   The Send Event to OpenNMS page appears.

2. From the Events field, select an event from the list.

3. To define the event and the network monitoring destination, specify appropriate values for the following fields:

- Node ID field—Select a device node from the list. The Node ID specifies the device in the event sent to the network monitoring system.
- Source Hostname—Specify the hostname of the source from which the event is sent.
- Interface field—Select the interface address to which the event is sent.
- Service field—Specify the name of the service that will receive the event.
- Parameters—Click the **Add additional parameters** link to specify the name and value of each additional parameter you want to add.
- Description field—Provide a description for the event.
- Severity field—Select a severity level for the event.
- Operator instructions—Include instructions that the operator might need to respond to the event notification.

4. Click **Send Event** to send the event to the system.

Managing Events Configuration Files

IN THIS SECTION

- Adding New Events Configuration Files | **841**
- Deleting Events Configuration Files | **842**
- Modifying Events Configuration Files | **842**

Adding New Events Configuration Files

To add a new events configuration file:

1. Select **Network Monitoring > Admin**.

   The Admin page is displayed.

2. Select **Manage Events Configuration** in the Operations section of the Admin page.

3. Click **Add New Events File**.

   The New Events Configuration pop-up window is displayed.

4. In the **Events File Name** field, enter a name for the events configuration file.

5. Click **Continue** to add the events configurations file.

Deleting Events Configuration Files

To delete an events configuration file:

1. Select **Network Monitoring > Admin**.

   The Admin page is displayed.

2. Select **Manage Events Configuration** in the Operations section of the Admin page.

3. From the **Select Events Configuration File** drop down menu, select the events configuration file you want to remove.

4. Click **Remove Selected Events File**.

5. Click **Yes**.

Modifying Events Configuration Files

You can edit the events in the events configuration XML file or add new events to this file.

1. Select **Network Monitoring > Admin**.

   The Admin page is displayed.

2. Select **Manage Events Configuration** in the Operations section of the Admin page.

3. From the **Select Events Configuration File** drop down menu, select the events configuration file you want to modify.

4. To add new events to this events configuration file:

   a. Click **Add Event**.

      Enter the new event details.

   b. In the **Event UEI** field, enter a unique event identifier.

   c. In the **Event Label** field, enter a label for the new event.

   d. In the **Description** field, enter a description for the new event.

e. In the **Log Message** field, enter a log message for the new event.

f. From the **Destination** drop down menu, select an appropriate option.

g. From the **Severity** drop down menu, select an appropriate option.

h. In the **Reduction Key** field, enter appropriate text.

i. In the **Clear Key** field, enter appropriate text.

j. From the **Alarm Type** drop down menu, select an appropriate option.

k. In the **Operator Instructions** field, enter instructions for the operator if required.

l. Click **Add** next to the **Mask Elements** table to add new element names and element values.

m. Click **Add** next to the **Mask Varbinds** table to add new varbind numbers and varbind values.

n. Click **Add** next to the **Varbind Decodes** table to add new parameter IDs and decode values.

o. Click **Save**.

5. To edit the current events configuration file:

   a. Select the event you want to edit.

   b. Scroll down to the bottom of the window and select **Edit**.

      You can now edit all the parameters of this event.

6. After you have added new events or modified the existing events, click **Save Events File**.

7. Click **Yes**.

RELATED DOCUMENTATION

Network Monitoring Workspace Overview | 799

CHAPTER 49

Managing and Configuring Alarms

IN THIS CHAPTER

- Viewing and Managing Alarms | 844
- Alarm Notification Configuration Overview | 857
- Configuring Alarm Notification | 860

Viewing and Managing Alarms

IN THIS SECTION

- Viewing Details of an Alarm and Acting on an Alarm | 846
- Viewing Alarms in Summary and Detailed Views | 849
- Viewing NCS Alarms | 855
- Searching for Alarms (Advanced Alarms Search) | 856

In the Network Monitoring workspace, events refer to any changes detected in the network. Network Monitoring allows you configure an event as an alarm by adding the **<alarm-data>** element to the event in the event configuration file. There are two categories of alarms: acknowledged and outstanding.

NOTE: An alarm that is cleared is removed from the Alarms page.

To search for and view information about alarms:

1. On the Junos Space Network Management Platform UI, select **Network Monitoring** > **Alarms**.

   The Alarms page appears.

2. (Optional) To view detailed information about an alarm:

   a. In the **Alarm ID** text box (in the **Alarm Queries** section), enter the ID for the alarm.

   b. Click **Get Details** or press Enter.

   - If the alarm ID that you entered matches an existing alarm, the subsequent page displays information about the alarm. For more information, see "Viewing Details of an Alarm and Acting on an Alarm" on page 846.
   - If the alarm ID that you entered does not match an existing alarm, the subsequent page displays a message to this effect.

3. (Optional) To view the list of all outstanding alarms:

   - Click the **All alarms (summary)** link (in the **Alarm Queries** section) to view a summarized list of alarms.

     The Alarms (List) page displays a summarized list of alarms in a table. For more information, see "Viewing Alarms in Summary and Detailed Views" on page 849.

   - Click the **All alarms (detail)** link (in the **Alarm Queries** section) to view a detailed list of alarms.

     The Alarms (List) page displays a detailed list of alarms in a table. For more information, see "Viewing Alarms in Summary and Detailed Views" on page 849.

4. (Optional) To search for alarms by specifying one or more search criteria, click the **Advanced Search** link (in the **alarm Queries** section).

   The **Advanced Alarm Search** page appears. For more information, see "Searching for Alarms (Advanced Alarms Search)" on page 856.

5. (Optional) To view the list of Network Communication Services (NCS) alarms, click the **NCS Alarm List** link.

   The Alarms (List) page appears with the search constraint **componentType="Service"** applied. For more information, see "Viewing NCS Alarms" on page 855.

6. (Optional) If alarm filter favorites were previously created, you can perform the following tasks in the **Alarm Filter Favorites** section:

   NOTE: You can view and delete only the alarm filter favorites that you created.

- View the constraints that are part of a filter by mousing over the information icon corresponding to a filter.

  The constraints are displayed in a window.

- View the alarms that match a filter by clicking the filter name link.

  The alarms (List) page where the list of alarms is displayed in a table. For more information, see "Viewing Alarms in Summary and Detailed Views" on page 849.

- Delete an alarm filter favorite by clicking the X link corresponding to the filter.

  The favorite is deleted and a message indicating that the favorite is deleted is displayed.

This topic has the following sections:

Viewing Details of an Alarm and Acting on an Alarm

On the Alarm *Alarm-ID* page, the details of an alarm, as shown in Table 112, are displayed. You can perform the following tasks on an alarm:

> **NOTE:** The background color for the fields on this page is the same color as the severity level of the alarm.

- Acknowledge the alarm—If an alarm has not been acknowledged, click the **Acknowledge** button (in the **Acknowledgment and Severity Actions** section) at the bottom of the page.

  The alarm is acknowledged and the details of the acknowledgment are displayed, as indicated in Table 112.

- Unacknowledge the alarm—If an alarm has been acknowledged but you want to unacknowledge it, click the **Unacknowledge** button (in the **Acknowledgment and Severity Actions** section) at the bottom of the page.

  The alarm is unacknowledged and the details of the unacknowledgment are displayed, as indicated in Table 112.

- Escalate the severity level of the alarm—Select **Escalate this alarm** from the list (in the **Acknowledgment and Severity Actions** section) at the bottom of the page and click **Go**.

  The alarm's severity level is escalated and the background color of the fields changes to match the severity level.

- Clear the alarm—Select **Clear this alarm** from the list (in the **Acknowledgment and Severity Actions** section) at the bottom of the page and click **Go**.

  The alarm's severity level is set to **Cleared** and the background color of the fields changes to match this severity level. When an alarm is marked to be cleared, the system removes the alarm after some time after which it is no longer available on the Alarms page.

Table 112: Details of an Alarm

Field	Description
Severity	Severity level of the alarm For details of the alarm severity levels, click the **Severity Legend** link on the Alarms (List) page.
Node	Node on which the alarm occurred You can click the node name link to view details about the node. Click the (+) icon to view the alarms only for this node on the Alarms page. Click the (–) icon to remove the alarms for this node from the Alarms page. The appropriate search constraint is applied when you click the (+) or (–) icon. Click the (–) icon in the **Search Constraints** field (top-left corner of the page) to remove the search constraint.
Last Event	Date and time of the last event for which the alarm was raised You can click the ***date and time*** link to view the details of the event.
Interface	Interface on which the alarm occurred You can click the ***Interface*** link to view details about the interface.
First Event	Date and time of the first event for which the alarm was raised
Service	Service for which the alarm was raised You can click the ***Service*** link to view details about the service.
Count	Number of times that the alarm was raised
UEI	Unique event identifier (UEI) associated with the alarm
Ticket ID	If configured by the user, the ID of ticket in the third-party ticket-based tracking system
Ticket State	If configured by the user, the state of the ticket in the third-party ticket-based tracking system
Reduction Key	Reduction key for the event If an alarm was raised for a previous event with the same reduction key, then a new alarm is not generated; only the alarm count is incremented.
Log Message	Message that was logged for the event for which the alarm was raised

Table 112: Details of an Alarm *(continued)*

Field	Description
Acknowledged By	If the alarm was acknowledged or unacknowledged, the username of the user who acknowledged or unacknowledged the alarm is displayed **NOTE:** If a remote user has cleared, acknowledged, escalated, or unacknowledged an alarm, the detailed alarm view displays *admin* instead of the actual remote user in the Acknowledged By field.
Acknowledged Type	Indicates whether the alarm was acknowledged or unacknowledged
Time Acknowledged	Date and time when the alarm was acknowledged or unacknowledged
Description	Detailed description of the event for which the alarm was raised.
Alarm History	If the alarm count is greater than 1 and the alarms have the same UEI, the alarm history is displayed in a table with the following information for each alarm: • **Event ID**—ID of the event associated with the alarm • **Alarm ID**—ID of the alarm • **Creation Time**—Date and time when the alarm was created • **Severity**—Severity of the alarm • **Operation Time**—Date and time when the operation occurred • **User**—Username of the user who performed the operation • **Operation**—Type of operation performed (**Escalate**, **Acknowledge**, or **Clear**)
Sticky Memo	If a sticky memo already exists, it is displayed in the text box. Below the text box, the author who created the memo, the date and time when the memo was last updated, and the date and time when the memo was created are displayed. • To add or modify a sticky memo, enter the note in the text box and click **Save**. The sticky memo is saved. • To delete a sticky memo, click **Delete**. The sticky memo is deleted. **NOTE:** A sticky memo is a user-defined note for a specific alarm; deleting an alarm also deletes the sticky memo.

Table 112: Details of an Alarm *(continued)*

Field	Description
Journal Memo	If a journal memo already exists, it is displayed in the text box. Below the text box, the author who created the memo, the date and time when the memo was last updated, and the date and time when the memo was created are displayed. • To add or modify a journal memo, enter the note in the text box and click **Save**. The journal memo is saved and applied to all alarms that share the same resolved reduction key as the alarm for which the journal memo was created. • To delete a journal memo, click **Delete**. The journal memo is deleted from all alarms that have the same resolved reduction key. **NOTE:** A journal memo is a user-defined note that is applicable to alarms that share the same resolved reduction key. Therefore, unlike in the case of a sticky memo, deleting an alarm does not delete the journal memo.
Operator Instructions	Instructions for the operator of the node on which the alarm occurred

Viewing Alarms in Summary and Detailed Views

By default, the Alarms (List) page displays the list of outstanding alarms in a table. However, depending on whether you used Advanced Search or applied a favorite filter, the list of alarms displayed might be different. For each alarm, the information shown in Table 113 is displayed.

You can filter and sort the list of alarms displayed based on various criteria:

1. (Optional) To apply an existing favorite alarm filter, select the name of the filter from the **Filter Name** list.

   The alarms are displayed based on the filter that you applied.

2. (Optional) If you applied a favorite alarm filter, you can remove it by clicking the **Remove Filter** button.

   All outstanding alarms are displayed on the Alarms (List) page.

3. (Optional) To search for alarms:

   NOTE: You must specify one of the search criteria.

   a. Enter the text (non-case-sensitive) in the **Alarm Text** field to search for alarms based on the text in the alarm log message.

b. From the **Time** list, select the period for which you want to view the alarms.

c. Click **Search**.

The outstanding alarms that match the search criteria are displayed. The search criteria is displayed in the **Search constraints** field.

4. (Optional) To view a specified number of alarms per page, select the required number from the list next to the **Results** field.

   By default, the number of alarms listed on the View Alarms page is 20. You can select the number of alarms you want to view per page from the **Show** list. You can choose to view 10, 20, 50, 100, 250, 500, or 1000 alarms.

   > **NOTE:** The number of alarms selected is set as user preference and the selected number of alarms are listed beginning from the next login.

5. (Optional) To sort the alarms displayed:
   - In descending order, click the column name link in the table once.
   - In ascending order, click the column name link in the table twice.

   The alarms are sorted based on the column that you clicked.

6. (Optional) To filter alarms based on different constraints:
   - To filter alarms on the basis of UEI, severity, node, interface, or service, click the plus (+) icon to view alarms only for the corresponding parameter or click the minus (–) icon to exclude alarms for the corresponding parameter.
   - To filter alarms on the basis of the date and time when the first event or last event for which the alarm was raised occurred, click the back arrow icon to view alarms that occurred after the corresponding date and time or click the forward arrow icon to view alarms that began before the corresponding date and time.
   - To filter alarms on the basis of the node from which they are triggered, click the (+) icon in the Node column. The Alarms page is filtered accordingly.

     Click the (–) icon to remove the alarms from a node on the Alarms page.

   The alarms in the table are displayed based on the constraints that you applied. In addition, the constraints that you applied are displayed in the **Search constraints** field.

7. (Optional) You can remove existing search constraints by clicking the minus (–) icon corresponding to a constraint in the **Search Constraints** field.

> **NOTE:** The **Alarms(s) outstanding** constraint is applied by default and cannot be removed. You can toggle this constraint with the **Alarm(s) acknowledged** constraint, which displays the list of acknowledged alarms, by clicking the minus (–) icon.

8. (Optional) To save a filter as a favorite:

> **NOTE:** You can save a filter as a favorite only if the filter contains search constraints other than **Alarm(s) outstanding** or **Alarm(s) acknowledged**.

   a. Click the **Save Filter** button in the **Search Constraints** field.

      A window is displayed instructing you to enter the name of the favorite filter.

   b. Enter a unique name (up to 30 alphanumeric characters except %, &, or #) for the filter in the text box.

   c. Click **OK**.

      - If an existing favorite filter has the same name, a warning message is displayed on the Alarms (List) page. You must enter a unique name to save the filter.
      - If the filter name that you specified is unique, the filter is saved and the Alarms (List) page appears. The **Filter Names** list displays the name of the filter.

> **NOTE:** Previously saved alarm filter favorites are accessible from the **Alarm Filter Favorites** section of the Alarms page.

9. (Optional) To view all outstanding alarms, click the **View all alarms** link at the top of the page.

   The Alarms (List) page displays the outstanding alarms.

10. (Optional) To search for alarms based on multiple criteria, click the **Advanced Search** link at the top of the page.

    The **Advanced Alarm Search** page appears. For more information, see "Searching for Alarms (Advanced Alarms Search)" on page 856

11. (Optional) To toggle between the summary and detailed views on the Alarms (List) page:

    - Click the **Long Listing** link to view the detailed view.

- Click the **Short Listing** link to view the summary view.

12. (Optional) To view the alarm severity levels, their color-coding, and explanation, click the **Severity Legend** link at the top of the page.

    The severity levels are displayed in a pop-up window. Click the Close (x) button to close the window.

13. (Optional) To acknowledge, unacknowledge, clear, or escalate one or more alarms:

    a. Select one or more alarms by selecting the check box corresponding to the alarm.

    > **NOTE:** You can select all alarms on the page by clicking the **Select All** button or clear the check boxes by clicking the **Reset** button; both buttons appear at the bottom of the page.

    b. To perform an action on the alarms selected:

        i. Do one of the following:

        - To acknowledge alarms, select **Acknowledge Alarms** from the list at the bottom of the page.

        > **NOTE:** This option is visible on the list only if one of the search constraints is **Alarm(s) outstanding**.

        - To unacknowledge alarms, select **Unacknowledge Alarms** from the list at the bottom of the page.

        > **NOTE:** This option is visible on the list only if one of the search constraints is **Alarm(s) acknowledged**.

        - To clear alarms, select **Clear Alarms** from the list.
        - To escalate alarms by one severity level, select **Escalate Alarms** from the list.

        ii. Click the **Go** button.

        The action that you selected is performed.

14. To acknowledge the entire list of outstanding alarms, click the **Acknowledge entire search** link.

    The alarms are processed in a batch and the **Acknowledged By**, **Acknowledged Type**, **Time Acknowledged** fields are updated for each alarm.

NOTE: This link is displayed only when outstanding alarms are displayed.

NOTE: If the list of alarms displayed runs across multiple pages, you can use the navigation links in the **Results** field near the top of the page to view the events.

Table 113: Fields Displayed on the Alarms (List) Page

Field	Description	Displayed In
Ack	Check box to select an alarm or clear a previously selected alarm When you select an alarm using the **Ack** check box, the possible actions are acknowledging, clearing, or escalating the alarm. **NOTE:** This check box is displayed when outstanding alarms are displayed on the Alarms (List) page.	Alarms (List) page (Short Listing) Alarms (List) page (Long Listing)
Unack	Check box to select an alarm or clear a previously selected alarm When you select an alarm using the **Ack** check box, the possible actions are acknowledging, clearing, or escalating the alarm. **NOTE:** This check box is displayed when previously acknowledged alarms are displayed on the Alarms (List) page.	Alarms (List) page (Short Listing) Alarms (List) page (Long Listing)
ID	Alarm ID You can click the *ID* link to view details of the alarm.	Alarms (List) page (Short Listing) Alarms (List) page (Long Listing)
Severity	Severity level of the alarm **NOTE:** The severity level of the alarm is displayed on a colored bar in the row. For information about the color-coding, click the **Severity Legend** link at the top of the page.	Alarms (List) page (Short Listing) Alarms (List) page (Long Listing)

Table 113: Fields Displayed on the Alarms (List) Page *(continued)*

Field	Description	Displayed In
UEI	**NOTE:** Only the **UEI** label is displayed on this page with options to filter based on the UEI.	Alarms (List) page (Long Listing)
Sticky Memo (Icon)	If a sticky memo exists for an alarm, an icon is displayed in the **ID** column. Mouse over the icon to view the memo.	Alarms (List) page (Short Listing) Alarms (List) page (Long Listing)
Journal Memo (Icon)	If a journal memo exists for an alarm, an icon is displayed in the **ID** column. Mouse over the icon to view the memo.	Alarms (List) page (Short Listing) Alarms (List) page (Long Listing)
Node	Node on which the alarm occurred You can click the node name link to view details about the node.	Alarms (List) page (Short Listing) Alarms (List) page (Long Listing)
Interface	Interface on which the alarm occurred You can click the interface link to view details about the interface.	Alarms (List) page (Long Listing)
Service	Service for which the alarm was raised You can click the ***Service*** link to view details about the service.	Alarms (List) page (Long Listing)
Count	Number of times that the alarm was raised You can click the count link to view the list of events for which the alarm was raised.	Alarms (List) page (Short Listing) Alarms (List) page (Long Listing)
Last Event Time	Date and time of the last event for which the alarm was raised You can click the ***date and time*** link to view the details of the event.	Alarms (List) page (Short Listing)
First Event Time	Date and time of the first event for which the alarm was raised	Alarms (List) page (Long Listing)
Acknowledged By	If the alarm was acknowledged or unacknowledged, the username of the user who acknowledged or unacknowledged the alarm is displayed.	Alarms (List) page (Long Listing)

Table 113: Fields Displayed on the Alarms (List) Page *(continued)*

Field	Description	Displayed In
Description	Detailed description of the alarm	Alarms (List) page (Short Listing) Alarms (List) page (Long Listing)
Log Message	Message that was logged for the alarm	Alarms (List) page (Short Listing) Alarms (List) page (Long Listing)

Viewing NCS Alarms

The Alarms (List) page with the search constraint **componentType="Service"** applied displays the list of NCS alarms in a table, as shown in Table 114. For more information about the actions that you can take on this page, see "Viewing Alarms in Summary and Detailed Views" on page 849.

Table 114: Fields in the NCS Alarms (List) Page

Field	Description
Ack	Refer to Table 113 for an explanation of this field.
Unack	Refer to Table 113 for an explanation of this field.
ID	Refer to Table 113 for an explanation of this field.
Severity	Refer to Table 113 for an explanation of this field.
Component Type	Type of component affected by the event (service, service element, or service element component)
Component Name	Name of the service for which the NCS alarm was raised
Related	Related services or component names (for example, VPN or Connectivity Fault Management Maintenance Endpoint [CFM-MEP]) impacted due to the event
Cause	Details of the event for which the NCS alarm was raised
Node	Refer to Table 113 for an explanation of this field
Last Event Time	Refer to Table 113 for an explanation of this field
Log Message	Refer to Table 113 for an explanation of this field

Searching for Alarms (Advanced Alarms Search)

On the Advanced Alarm Search page, you can search for alarms using several criteria.

To search for alarms:

1. (Optional) In the **Alarm Text Contains** field, enter the text (partial or full) that you want to search for.

   The text that you entered is matched against the **Log Message** field of the alarm.

2. (Optional) In the **TCP/IP Address Like** field, enter the interface IP address in the *.*.*.* format for IPv4 addresses and *:*:*:*:*:*:*:* for IPv6 addresses.

3. (Optional) In the **Node Label Contains** field, enter the name of the node (partial or full).

4. (Optional) Specify the severity of the alarm using the **Severity** list.

5. (Optional) Select the service for which the alarm was raised from the **Service** list.

6. (Optional) To search for alarms for which the first event occurred after a specified date and time, specify the date and time in the **Alarm First Event After** field.

   > **NOTE:** If you want to search for alarms within a certain date and time range, you can use a combination of the **Alarm First Event After**, **Alarm First Event Before**, **Alarm Last Event After**, and **Alarm Last Event Before** fields.

7. (Optional) To search for alarms for which the first event occurred before a specified date and time, specify the date and time in the **Alarm First Event Before** field.

8. (Optional) To search for alarms for which the last event occurred after a specified date and time, specify the date and time in the **Alarm Last Event After** field.

9. (Optional) To search for alarms for which the last event occurred before a specified date and time, specify the date and time in the **Alarm Last Event Before** field.

10. (Optional) Specify a sorting order for the search results using the **Sort By** list.

    By default, search results are sorted in descending order of alarm ID.

11. (Optional) Specify the number of alarms to display per page using the **Number of Alarms Per Page** list.

12. Click **Search** or press Enter when your cursor is inside one of the text boxes.

    The Alarms (List) page appears displaying the alarms that match your search parameters are displayed. For more information, see "Viewing Alarms in Summary and Detailed Views" on page 849

RELATED DOCUMENTATION

Viewing, Configuring, and Searching for Notifications | 865

Viewing and Managing Events | 833

Searching for Nodes or Nodes with Asset Information | 816

Alarm Notification Configuration Overview

IN THIS SECTION

- Basic Filtering | 857
- Guidelines for Configuring Alarm Notifications | 858
- Advanced Filtering | 859

By default, the alarms generated by managed devices in the Junos Space platform are sent to the network monitoring functionality. To enable alarm notification for supported Junos Space applications, you can configure the **alarmNotificationConf.xml** file to specify the alarm notifications that designated Junos Space applications should receive. The applications will receive only those alarms that you configure in the **alarmNotificationConf.xml** file and that match the specified filter criteria.

You can configure basic and advanced filters so that any alarms that match the configured filtering conditions are forwarded to the designated applications.

Basic Filtering

You configure a basic filter to filter alarms based on the Unique Event Identifier (UEI), device family, and severity. At minimum, you must configure a UEI filter. Filtering by device family, severity, or both, is optional.

To configure a basic filter for alarm notification, at minimum, you must configure the following notification tags in the **alarmNotificationConf.xml** file, which must reside in the **/opt/opennms/etc/alarm-notification** directory:

- Notification name
- UEI of the alarm to be notified
- The script to be executed for the configured UEI

You can also configure the following tags in the **alarmNotificationConf.xml** file:

- Severity—Supported severity values are Indeterminate, Cleared, Normal, Warning, Minor, Major, and Critical.

  When configuring an alarm for notification, a notification is sent for the corresponding Clear Alarm. A notification is also sent after clearing an alarm from the user interface. To forward notification for Clear alarms and user interface (UI) , you must configure **Severity = Normal, Cleared**.
- Device Family—Supported device family is present in the **devicefamily.properties** in the **/opt/opennms/etc/alarm-notification**.

  NOTE: If the Sysoid for the device is unknown, the **DevicesWithNoSysoid** filter is matched.

Guidelines for Configuring Alarm Notifications

Use the following guidelines when configuring alarm notifications:

- To send notification when an alarm is cleared from the UI, you must include **event uei.opennms.org/vacuumd/juniper/alarmCleared** in the **eventconf.xml** file.
- The event entry is present in **/opt/opennms/etc/examples/alarm-notification/eventconf.xml**. This entry should be added to **/opt/opennms/etc/eventconf.xml**.

  NOTE: Do not copy and paste the entire **/opt/opennms/etc/examples/alarm-notification/eventconf.xml** file. If the event entry is not already present, append the event entry to the existing **eventconf.xml** file.

- The tags listed in the **/opt/opennms/etc/examples/alarm-notification/vacuumd-configuration.xml** file should be added to the **/opt/opennms/etc/vacuumd-configuration.xml** file, if not already present.
- Alarm notification dampening is performed based on the alarm counter. The **notification_threshold** attribute is added for this purpose. The default value is 5, which specifies that the first alarm is notified, then the sixth alarm, and so on.

Advanced Filtering

To provide more in-depth filtering, you must configure a drool (DRL) file. With advanced filtering, the applications receive only those alarms that match all the advanced filtering conditions. The name of the drool file and notification name mentioned in the **alarmNotificationConf.xml** file should match, and for each notification, there must be a drool file whose name matches the notification name. Each drool file that you configure must be added to the **/opt/opennms/etc/alarm-notification/drools** directory. You can view a sample drool file from the **/opt/opennms/etc/examples/alarm-notification/drools** directory. You can view a sample **alarmNotification.xml** file from the **/opt/opennms/etc/examples/alarm-notification** directory.

> **NOTE:** Care should be taken when writing the rule. For each rule that satisfies the condition, a corresponding script is invoked. For better performance, do not configure multiple rules for the same UEI.

You can create advanced filters based on any combination of the following fields:

- alarmacktime
- alarmackuser
- alarmid
- alarmtype
- applicationdn
- clearkey
- counter
- description
- dpname
- eventparms
- eventuei
- firsteventtime
- ifindex
- ifname
- ipaddr
- lasteventtime
- logmsg
- ossprimarykey

- operinstruct
- reductionkey
- serviced
- severity
- suppressedtime
- suppresseduntil
- suppresseduser
- tticketid
- tticketstate
- uiclear
- x733Alarmtype
- x733Probablecause

RELATED DOCUMENTATION

Configuring Alarm Notification | 860

Configuring Alarm Notification

IN THIS SECTION

- Configuring a Basic Filter for Alarm Notification | 861
- Activating Alarm Notification Configuration Files for Basic Filtering | 863
- Reloading a Filter Configuration to Apply Filter Configuration Changes | 863

By default, the alarms generated by managed devices in the Junos Space platform are sent to the network monitoring functionality. To enable alarm notification for supported Junos Space applications, you can

configure alarm notification files for basic filtering to specify the alarm notifications that designated Junos Space applications should receive.

Configuring a Basic Filter for Alarm Notification

The following steps show how to configure a basic filter based on unique event identifier (UEI), severity, and device family. When the alarm criteria specified in the XML file are matched, the alarm XML is passed as an argument to the invoked script.

To configure a basic filter for alarm notification:

1. Configure the destination for the notification in the script, for example, **Sample_App_Script.sh**. The script specifies how the alarm notifications are sent to the application.

```
curl -v -u super:juniper123 -X POST -H  "Content-Type:application/xml" -d "$xml"
 "http://localhost:8080/SampleApplication/services/Alarms"
```

> **NOTE:** In the preceding example, the curl command is used to post the script, but the configuration of the script can vary based on the requirements of the application.
>
> You can access sample configuration scripts from the **/opt/opennms/etc/examples/alarm-notification/scripts** directory. However, all active scripts must be present in the **/opt/opennms/etc/alarm-notification/scripts** directory.

2. In the **alarmNotificationConf.xml** configuration file:
   a. Enable the alarm notification feature:

```
<notification name="SampleAppNotification" enable="true">
```

   b. Configure the number of seconds to wait for the script to execute before timing out:

```
<script timeout_in_seconds=”45”>
```

> **NOTE:** If you do not configure the **timeout_in_seconds** attribute, the default time out for the script invoked is 60 seconds. In this case, the shell exit status will be '143' and error handling will be considered in the same way as other error exit status. If the script continues to execute after the timeout value for the script, alarm notification will not wait for the script status. During this time, processing of other alarms will not be blocked.

c. Specify the name of the script that will be invoked:

```
<scriptname>Sample_App_Script.sh</scriptname>
```

The configured script must be present in the **/opt/opennms/etc/alarm-notification/scripts** directory.

d. Enable error handling, and configure the number of notification retry attempts and interval (in seconds) between retry attempts, if the initial attempt to send the notification fails:

```
<errorhandling enable="true">
     <retry_interval_inseconds>3</retry_interval_inseconds>
    <number_of_retries>2</number_of_retries>
</errorhandling>
```

> **NOTE:** The script exit status should be '0' if there are no errors. For other exit status values, the script will be invoked again if error handling is enabled.

e. Configure the UEI of the alarms which will require notification:

```
<uies>
     <uei name="uei.opennms.org/generic/traps/SNMP_Link_Down"
notification_threshold=”5”
          <filter devicefamily=”JSeries” severity=”Minor,Normal”/>
         <filter devicefamily=”DevicesWithNoSysoid"  severity=”Minor,Normal”/>
     <uei/>
</uies>
```

Activating Alarm Notification Configuration Files for Basic Filtering

After configuring the alarm notification files for basic filtering, you must add the files to the Junos Space application to activate the alarm notification configuration:

1. Log in from the Junos Space system console.

   The Junos Space Appliance Settings menu displays.

2. From the Junos Space Appliance Settings menu, enter **7** (or enter **8** from the Junos Space Virtual Appliance) to run the shell.

3. (Optional): To view the sample configuration files for alarm notification:

   - Navigate to the **/opt/opennms/etc/examples/alarm-notification** directory to view sample files for **alarmNotificationConf.xml**, **eventconf.xml**, and **vacuumd-configuration.xml**.

   - Navigate to the **/opt/opennms/etc/examples/alarm-notification/scripts** directory to view the **CBU_App_Script.sh** and **NA_App_Script.sh** sample scripts.

4. To activate configuration files for alarm notification, perform the following steps:

   a. Add your configured **alarmNotificationConf.xml** file to the **/opt/opennms/etc/alarm-notification** directory.

   b. Add your configured **eventconf.xml** and **vacuumd-configuration.xml** files to the **/opt/opennms/etc** directory.

   c. Add your configured script file to the **/opt/opennms/etc/alarm-notification/scripts** directory.

Reloading a Filter Configuration to Apply Filter Configuration Changes

After making any changes to a filter, you can reload the configuration by sending a “reloadDaemonConfig” event, for example:

```
/opt/opennms/bin/send-event.pl -p 'daemonName Alarmd.AlarmNorthbounder'
  uei.opennms.org/internal/reloadDaemonConfig
```

You do not need to restart the server to apply the configuration changes listed in previous steps. However, to send the event, go to **/opt/opennms/bin ./send-event.pl -p 'daemonName Alarmd.AlarmNorthbounder' uei.opennms.org/internal/reloadDaemonConfig**.

This event will reload the following files:

- **alarmNotficationConf.xml**
- **devicefamily.properties**
- Drool (**.drl**) files

RELATED DOCUMENTATION

Alarm Notification Configuration Overview | **857**

CHAPTER 50

Managing and Configuring Notifications

IN THIS CHAPTER

- Viewing, Configuring, and Searching for Notifications | 865
- Configuring Event Notifications, Path Outages, and Destination Paths | 867

Viewing, Configuring, and Searching for Notifications

IN THIS SECTION

- Notification Escalation | 866

When the system detects important events, one or more notices are sent automatically to configured notification information (such as a pager, an e-mail address, or other notification methods). In order to receive notices, users must have their notification information configured in their user profile (see "Configuring Network Monitoring System Settings" on page 901), notices must be switched on, and an important event must be received.

Select **Network Monitoring > Notifications**. From the Notifications page, you can:

- Display all unacknowledged notices sent to your user ID by clicking **Your outstanding notices**.
- View all unacknowledged notices for all users by clicking **All outstanding notices**.
- View a summary of all notices sent and acknowledged for all users by clicking **All acknowledged notices**.
- Search for notices associated with a specific user ID by entering that user ID in the User field and clicking **Check notices**.
- Jump immediately to a page with details specific to a given notice identifier by entering that numeric identifier in the Notice field and clicking **Get details**.

> **NOTE:** Getting details is particularly useful if you are using a numeric paging service and receive the numeric notice identifier as part of the page.

Notification Escalation

Once a notice is sent, it is considered outstanding until someone acknowledges receipt of the notice using the Notice *notice ID* section of the Notifications page. Select **Network Monitoring > Notifications**, enter a notice ID in the Notice field, click **Get details**, and click **Acknowledge**.

If the event that triggered the notice was related to managed network devices or systems, the Network/Systems group is notified, one by one, with a notice sent to the next member on the list only after 15 minutes has elapsed since the last message was sent.

This progression through the list, or escalation, can be stopped at any time by acknowledging the notice. Note that this is not the same as acknowledging the *event* that triggered the notice. If all members of the group have been notified and the notice has not been acknowledged, the notice is escalated to the Management group, where all members of that group are notified simultaneously (with no 15-minute escalation interval). For details on configuring groups, see "Configuring Network Monitoring System Settings" on page 901.

RELATED DOCUMENTATION

- Network Monitoring Workspace Overview | **799**
- Viewing the Node List | **809**
- Viewing Managed Devices | **194**
- Resynchronizing Nodes in Network Monitoring | **813**
- Searching for Nodes or Nodes with Asset Information | **816**

Configuring Event Notifications, Path Outages, and Destination Paths

IN THIS SECTION

- Configuring Event Notifications | 867
- Configure Destination Paths | 869
- Configure Path Outages | 871

Configuring Event Notifications

You can configure an event to send a notification whenever that event is triggered. You can add, edit, and delete event notifications.

To add a notification to an event:

1. Select **Network Monitoring > Admin > Configure Notifications > Configure Event Notifications**.
2. Click **Add New Event Notification**.
3. Select the event UEI that will trigger the notification.
4. Click **Next**.
5. Build the rule that determines whether to send a notification for this event, based on the interface and service information specified in the event.
6. You can validate the rule results or skip the rule results validation:
   - To validate the rule results:
     a. Click **Validate rule results** and click **Next** after reviewing the results..

        Alternatively, you can skip the validate rule results step and click **Skip results validation**.

        The Choose the destination path and enter the information to send via the notification page appears.

     b. Specify a name for the notification, choose the destination path, and enter the information required to send with the notification.

        You can include the following values in the text message, short message, and the E-mail subject:

- **%noticeid%** to include the notification ID number.
- **%nodelabel%** to include the node label as an IP address.
- **%eventid%** to include the event ID.
- **%ifalias%** to include the SNMP IF alias of the affected interface.
- **%time%** to indicate the time when the notification was sent.
- **%interface%** to include the IP address of the interface.
- **%parm[a_parm_name]%** to include the name, if any, of the event parameter.
- **%interfaceresolve%** to include the reverse DNS name of the interface IP address.
- **%severity%** to include the severity of the event.
- **%service%** to include the name of the service.
- **%parm[#N]%** to include the value of the event parameter at index N.
- **%operinstruct%** to include the operator instructions from the event definition.

c. Click **Finish**.

To edit an existing event notification:

1. Select **Network Monitoring > Admin > Configure Notifications > Configure Event Notifications**.
2. Click the **Edit** button that is located to the left of the event notification you want to modify.
3. Select the event UEI that will trigger the notification.
4. Click **Next**.
5. Build the rule that determines whether to send a notification for this event, based on the interface and service information specified in the event.
6. (Optional) Click **Reset Address and Services** if you want to clear the changes that you have entered.
7. You can validate the rule results or skip the rule results validation:
   - To validate the rule results:
     a. Click **Validate rule results** and click **Next** after reviewing the results..

        Alternatively, you can skip the validate rule results step and click **Skip results validation**.

        The Choose the destination path and enter the information to send via the notification page appears.

b. Specify a name for the notification, choose the destination path, and enter the information required to send with the notification.

   The Choose the destination path and enter the information to send via the notification page appears.

   You can include the following values in the text message, short message, and the E-mail subject:

   - **%noticeid%** to include the notification ID number.
   - **%nodelabel%** to include the node label as an IP address.
   - **%eventid%** to include the event ID.
   - **%ifalias%** to include the SNMP IF alias of the affected interface.
   - **%time%** to indicate the time when the notification was sent.
   - **%interface%** to include the IP address of the interface.
   - **%parm[a_parm_name]%** to include the name, if any, of the event parameter.
   - **%interfaceresolve%** to include the reverse DNS name of the interface IP address.
   - **%severity%** to include the severity of the event.
   - **%service%** to include the name of the service.
   - **%parm[#N]%** to include the value of the event parameter at index N.
   - **%operinstruct%** to include the operator instructions from the event definition.

c. Click **Finish**.

To delete an existing event notification:

1. Select **Network Monitoring > Admin > Configure Notifications > Configure Event Notifications**.
2. Click the **Delete** button that is located to the left of the event notification you want to modify.
3. Click **Ok** in the delete notification confirmation dialog box to delete the notification.

Configure Destination Paths

You can configure a destination path that describes what users or groups will receive notifications, how the notifications will be sent, and who to notify if escalation is needed. A destination path defines a reusable list of contacts that you include in an event configuration.

To create a new destination path:

1. Select **Network Monitoring > Admin > Configure Notifications > Configure Destination Paths**.
2. Click the **New Path** button.
3. Specify appropriate values for the following fields:
   - Name—Specify a name for the destination path.
   - Initial Delay—From the list, select the number of seconds to wait before sending notifications to users or groups.
   - Initial targets—Select the users and groups to whom the event notification will be sent.
4. Click the **Add Escalation** button to specify users and groups to whom event notification will be sent.
5. Choose the commands to use (for example, callHomePhone, callMobilePhone, or callMobilePhone) for each user and group.
6. Click **Next**.
7. Click **Finish** when you have finished editing the destination path.

To modify an existing destination path:

1. Select **Network Monitoring > Admin > Configure Notifications > Configure Destination Paths**.
2. Under Existing Paths, select the existing destination path that you want to modify.
3. Click **Edit**.
4. You can make changes to any of the following fields:
   - Initial Delay—From the list, select the number of seconds to wait before sending notifications to users or groups.
   - Initial targets—Add users and groups to whom the event notification should be sent and remove users and groups to whom the event should not be sent.
5. Click the **Add Escalation** button to specify users and groups to whom event notification will be sent.
6. Choose the commands to use (for example, callHomePhone, callMobilePhone, or callMobilePhone) for each user and group.

7. Click **Next**.

8. Click **Finish** when you have finished modifying the destination path.

To delete a destination path:

1. Select **Network Monitoring > Admin > Configure Notifications > Configure Destination Paths**.

2. Under Existing Paths, select the existing destination path that you want to delete.

3. Click **Delete**.

4. Click **Ok** to confirm that you want to delete the selected destination path.

Configure Path Outages

You can configure a path outage that describes what users or groups will receive notifications, how the notifications will be sent, and who to notify if escalation is needed. A destination path defines a reusable list of contacts that you include in an event configuration.

To create a new path outage:

1. Select **Network Monitoring > Admin > Configure Notifications > Configure Path Outage**.

2. Click the **New Path** button.

3. Specify appropriate values for the following fields:
   - Critical Path—Enter the critical path IP address.
   - Critical Path Service—From the list, select the ICMP protocol.
   - Initial targets—Select the users and groups to whom the event notification will be sent.
4. Build the rule that determines which nodes are subject to this critical path.

5. Select the **Show matching node list** check box to show the list of nodes that match.

6. Choose the commands to use (for example, callHomePhone, callMobilePhone, or callMobilePhone) for each user and group.

7. Click **Validate rule results** to validate the rule.

8. Click **Finish** when you have finished configuring the path outage.

RELATED DOCUMENTATION

Network Monitoring Workspace Overview | 799

CHAPTER 51

Managing Reports and Charts

IN THIS CHAPTER

- Network Monitoring Reports Overview | 873
- Creating Reports | 874
- Viewing Reports | 876
- Deleting Reports | 881
- Viewing Charts | 883

Network Monitoring Reports Overview

IN THIS SECTION

- Resource Graphs | 873
- Key SNMP Customized Performance Reports, Node Reports, and Domain Reports | 874
- Database Reports | 874
- Statistics Reports | 874

You can generate and view resource graphs, key SNMP customized (KSC) performance reports, KSC node reports, KSC domain reports, database reports, and statistics reports. To access the reports function, select **Network Monitoring > Reports**.

Resource Graphs

Resource graphs provide an easy way to represent visually the data collected from managed nodes throughout your network. You can display critical SNMP performance, response time, and so forth.

You can narrow your selection of resources by entering a search string in the Name contains box. This invokes a case-insensitive substring match on resource names.

Key SNMP Customized Performance Reports, Node Reports, and Domain Reports

KSC reports enable you to create and view SNMP performance data using prefabricated graph types. The reports provide a great deal of flexibility in time spans and graph types. You can save KSC report configurations so that you can refer to key reports in the future.

Node reports show SNMP data for all SNMP interfaces on a node.

Domain reports show SNMP data for all SNMP interfaces in a domain. You can load node reports and domain reports into the customizer and save them as a KSC report.

You can narrow your selection of resources by entering a search string in the Name contains box. This invokes a case-insensitive substring match on resource names.

Database Reports

Database reports provide a graphical or numeric view of your service-level metrics for the current month-to-date, previous month, and last 12 months by categories.

Statistics Reports

Statistics reports provide regularly scheduled statistical reports on collected numerical data (response time, SNMP performance data, and so forth).

RELATED DOCUMENTATION

- Network Monitoring Workspace Overview | 799
- Creating Reports | 874
- Deleting Reports | 881
- Viewing Reports | 876
- Viewing the Node List | 809

Creating Reports

IN THIS SECTION

- Creating Key SNMP Customized Performance Reports, Node Reports, and Domain Reports | 875
- Creating a New KSC Report from an Existing Report | 875

You can configure key SNMP customized (KSC) performance reports, node reports, and domain reports by selecting **Network Monitoring > Reports**.

Creating Key SNMP Customized Performance Reports, Node Reports, and Domain Reports

To create a new KSC report:

1. Select **Network Monitoring > Reports > KSC Performance, Nodes, Domains**.
2. From the Node and Domain Interface Reports section, select a resource for the report.
3. Under the Customized Reports section, click **Create New > Submit**.

   The Customized Report Configuration page is displayed.
4. In the Title text box, enter a name for the report.
5. (Optional) To add a graph to the report:
   a. Select **Add New Graph**.
   b. Select a resource from the Resources section.
   c. Select **Choose Child Resource** to select the resource you want to use in a graph.
   d. Select the check box for the specific node resources you want to view, or click **Select All** to select all the displayed node resources.
6. (Optional) To allow global manipulation of the report timespan, select **Show Timespan Button**.
7. (Optional) To allow global manipulation of report prefabricated graph type, select **Show Graphtype Button**
8. (Optional) Select the number of graphs to show per line in the report.
9. To save the report, click **Save**.

Creating a New KSC Report from an Existing Report

To create a new KSC report from an existing report:

1. Select **Network Monitoring > Reports > KSC Performance, Nodes, Domains**.
2. Under the Resources section, select the KSC report that you want to use to create a new report and click **Create New from Existing > Submit**.

The Customized Report Configuration page is displayed.

3. Select a resource.

4. In the Title text box, enter a new name for the report.

5. (Optional) Customize the report by adding graphs and specifying the number of graphs per line.

6. Click **Save**.

RELATED DOCUMENTATION

- Network Monitoring Workspace Overview | **799**
- Network Monitoring Reports Overview | **873**
- Viewing Reports | **876**
- Deleting Reports | **881**
- Viewing the Node List | **809**
- Viewing Managed Devices | **194**

Viewing Reports

Select **Network Monitoring > Reports** to view the following types of reports:

- Resource graphs that provide SNMP performance data collected from managed nodes on your network
- Key SNMP customized (KSC) performance reports, node reports, and domain reports. You can generate KSC reports to view SNMP performance data using prefabricated graph types.
- Database reports that provide graphical or numeric views of service-level metrics.
- Statistics reports that provide regularly scheduled reports on response time, SNMP node-level performance and interface data, and OSPF area data.

Viewing Resource Graphs

To view a resource graph:

1. Select **Network Monitoring > Reports > Resource Graphs**.

2. Select the resource node for which you want to generate a standard performance report or custom performance report.

   The Node Resources page is displayed.

3. To select the specific node resources data that you want to view, choose one of the following options:
   - To view data for a subset of node resources:
     a. Click the **Search** option.
     b. Enter a text string to identify the node resources you want to view.
     c. Click **OK**.
     d. Select the check box for the specific node resources you want to view, or click **Select All** to select all the displayed node resources.
   - To view data for all listed node resources, click **Select All**.
4. To display graphical data for the all the selected node resources, click **Graph Selection**.

5. In the Time Period field, specify the period of time (last day, last week, last month, or custom) that the report should cover.

   The statistical data is refreshed to reflect the time period specified.

Viewing Key SNMP Customized (KSC) Performance Reports, Node Reports, and Domain Reports

To view a KSC report:

1. Select **Network Monitoring > Reports > KSC Performance, Nodes, Domains**.

2. Select the resource node for which you want to view a standard performance report or custom performance report.

   The Custom View Node Report is displayed.

3. (Optional) To customize the Node Report view:
   - To override the default time span, in the Override Graph Timespan list, select the number of hours, days, or months, or select by quarter, or year.

- To override the default graph type, from the Override Graph type list, select the number of hours, days or months, by quarter or by year.

4. Select **Update Report View** to refresh the report.

5. Select **Exit Report Viewer** to exit the report view, or select **Customize This Report** to make additional updates to the report.

Viewing Database Reports

To view database reports:

1. Select **Network Monitoring > Reports > Database Reports > List reports**.

   The Local Report Repository page is displayed.

2. Select on a report page number, or select **Next** or **Last** to scroll through the available reports to locate the database report you want to view.

3. To execute a report, from the row that lists the report, select the arrow icon from the Action column.

   The Run Online Report page is displayed.

4. In the Report Format field, select either PDF or comma-separated values (CSV) format for the report from the list.

5. Select **run report**.

   For PDF, the report is displayed in the selected format. For CSV, you are prompted to either open or save the file.

Sending Database Reports

To send database reports:

1. Select **Network Monitoring > Reports > Database Reports > List reports**.

   The Local Report Repository page is displayed.

2. Select on a report page number, or select **Next** or **Last** to scroll through the available reports to locate the database report you want to send.

3. You can send a report to file system or e-mail the report.

   - To execute a report, in the row that lists the report, select the arrow icon from the Action column.

The Run Online Report page is displayed.

a. From the Report Format list, select either PDF or comma-separated values (CSV) format for the report from the list.

b. Select **run report**.

   For PDF, the report is displayed in the selected format. For CSV, you are prompted to either open or save the file.

- To send a report to a file system or e-mail the report, select the Deliver report icon from the Action column.

  The Report Parameters page is displayed.

  a. From the report category field, select a category (Network Interfaces, Email Servers, Web Servers, Database Servers, and so forth).

  b. From the end date field, select the end date and time for the report.

  c. Select **Proceed**.

     The Report Delivery Options page is displayed.

  d. In the name to identify this report field, specify a name for the report.

  e. (Optional) To send the report through e-mail, select the e-mail report check box.

  f. In the format field, select the format type (HTML, PDF, or SVG).

  g. In the recipient field, enter the name of the person to whom the report will be sent.

  h. (Optional) To save a copy of the report select the **save a copy of this report** check box.

  i. Select **Proceed**.

     The Report Running page is displayed.

  j. Select **Finished** to close the page and return to the Local Report Repository page.

Viewing Pre-run Database Reports

To view database reports:

1. Select **Network Monitoring > Reports > Database Reports > View and manage pre-run reports**.

   All the pre-run reports are displayed in a table.

2. From the view report column, select the **HTML**, **PDF**, or **SVG** link to specify the format in which you want to view the report.

   The database report is displayed.

Viewing Statistics Reports

To view statistics reports:

1. Select **Network Monitoring > Reports > Statistics Reports**.

   The Statistics Report List page displays a list of all available reports in a table.

2. To search for specific information in statistics reports, enter search text in the blank field directly above a Statistics Report column, and select **Filter**.

   All available statistics reports that match the filter text you specified are displayed in the Statistics Report List page.

3. To clear the filtered information and restore the original list of statistics reports, select **Clear**.

   All available statistics reports are again displayed in the Statistics Report List page.

4. To view complete information for a specific statistics report, click the Report description link from the Statistics Report List page.

   The statistics report is displayed and includes Parent resources and resource graphs with SNMP interface data.

Generating a Statistics Report for Export

To generate a statistics report as a PDF file or Excel spreadsheet:

1. Select **Network Monitoring > Reports > Statistics Reports**.

   The Statistics Report List page displays a list of all available reports in a table.

2. In the Report Description column, select the report link.

The statistics report is displayed and includes all information for that report, including parent resources and resource graphs with SNMP interface data.

3. Choose PDF or Excel as the format for the statistics report:
   - To generate the statistics report in PDF format, in the top-right corner of the Statistics Report, select the **Export PDF** icon.

     The File Download window is displayed.
   - To generate the statistics report as an Excel spreadsheet, in the top-right corner of the Statistics Report, select the **Export Excel** icon.

     The File Download window is displayed.
4. From the File Download window, select **Open** to view the statistics report or select **Save** to save the statistics report.

RELATED DOCUMENTATION

- Network Monitoring Workspace Overview | 799
- Network Monitoring Reports Overview | 873
- Creating Reports | 874
- Deleting Reports | 881
- Viewing the Node List | 809
- Viewing Managed Devices | 194
- Resynchronizing Nodes in Network Monitoring | 813
- Searching for Nodes or Nodes with Asset Information | 816

Deleting Reports

IN THIS SECTION

- Deleting Key SNMP Customized Reports | 882
- Deleting Pre-Run Database Reports | 882

To delete key SNMP customized (KSC) reports and database reports, select **Network Monitoring > Reports**.

Deleting Key SNMP Customized Reports

To delete a KSC report:

1. Select **Network Monitoring > Reports > KSC Performance, Nodes, Domains**.
2. From the Customized Reports section, select the report that you want to delete.
3. Select the **Delete** radio button.
4. Select **Submit**.

   The KSC report is deleted.

Deleting Pre-Run Database Reports

To delete a database report:

1. Select **Network Monitoring > Reports > View and manage pre-run reports**.

   All the pre-run reports are displayed in a table.
2. From the select column in the reports table, select the check box for the database report that you want to delete.
3. Select **delete checked reports**.

   The database report is deleted.

RELATED DOCUMENTATION

- Network Monitoring Workspace Overview | **799**
- Network Monitoring Reports Overview | **873**
- Creating Reports | **874**
- Viewing Reports | **876**
- Viewing the Node List | **809**
- Viewing Managed Devices | **194**
- Resynchronizing Nodes in Network Monitoring | **813**
- Searching for Nodes or Nodes with Asset Information | **816**

Viewing Charts

To view charts, select **Network Monitoring > Charts**.

By default, this page displays:

- Alarms Severity Chart, showing the counts of both alarms and events, distinguishing between major, minor, and critical severities.
- Last 7 Days Outages, showing the counts of outages per service.
- Node Inventory, showing the counts of nodes, interfaces, and services.

CHAPTER 52

Network Monitoring Topology

IN THIS CHAPTER

- Network Monitoring Topology Overview | **885**
- Working with Topology | **887**
- Network Monitoring Topology Discovery Methods Supported by Junos Space Network Management Platform | **899**

Network Monitoring Topology Overview

On the Topology page in the Network Monitoring workspace, you can view Junos Space nodes, Fault Monitoring and Performance Monitoring (FMPM) nodes, and devices that were discovered by Junos Space Network Management Platform, as well as node links and the alarm state of the services links.

> **NOTE:** On the Topology page, the term *node* refers to Junos Space nodes, FMPM nodes, or devices discovered by Junos Space Network Management Platform. The term *node link* refers to the link between the nodes.

The EnhancedLinkd network topology discovery daemon is used to discover the network topology. Five physical link discovery methods—Bridge Discovery Protocol, Cisco Discovery Protocol (CDP), IS-IS, Link Layer Discovery Protocol (LLDP), and OSPF—are supported and enabled by default. After the SNMP interface is discovered, the availability of links in the topology depends on the following:

> **NOTE:** Junos Space Platform currently supports only OSPF version 2 for topology discovery.

- The time that the EnhancedLinkd daemon waits after a node has been provisioned; the default is 60 seconds
- The time taken for the EnhancedLinkd deamon to scan the node
- The time after which the node links are refreshed automatically; the default is 60 seconds

After the topology is discovered by Junos Space Platform, any changes to the topology are automatically detected. This includes changes in logical entities, such as Ethernet services and VPNs, that are discovered by Junos Space Platform. The EnhancedLinkd daemon updates only the topology changes in the database and does not rescan the entire network. This *incremental* link discovery ensures that data related to topology changes is updated dynamically. In addition, the dynamic update ensures that only the node or the node link that was updated is redrawn and not the entire topology.

NOTE:

- From Junos Space Network Management Platform Release 14.1R1 onward, the SNMP polling time for discovering links between devices is set using the **rescan_interval** parameter in the **enlinkd-configuration.xml** file. In prior releases, this SNMP polling time for discovering links between devices was set using the **snmp_polling** parameter in the **linkd.xml** file. The default value for the **rescan_interval** parameter is 86,400,000 milliseconds
- A sample of the **/opt/opennms/etc/enlinkd-configuration.xml** is as follows:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<linkd-configuration threads="5"
                     initial_sleep_time="60000"
                     rescan_interval="86400000"
                     use-cdp-discovery="true"
                     use-bridge-discovery="true"
                     use-lldp-discovery="true"
                     use-ospf-discovery="true"
                     use-isis-discovery="true"
                     />
```

For more information about the parameters in the **enlinkd-configuration.xml** file, see http://www.opennms.org/wiki/Linkd .

The node link status is color-coded—a green link indicates that the link is up and a red link indicates that a link is down. In addition, if an SNMP trap is received indicating that the node link status has changed, then the EnhancedLinkd daemon updates the node link in the topology to indicate the current status of the node link.

The alarm state of services links is also color-coded—a green line indicates that no service-impacted alarms are present and that the service status is up; a red line indicates that at least one service-impacted alarm is present and that the service status is down.

NOTE:

- The color-coding of the link status is displayed only if the option to display the link status is selected; this option is *not* selected by default.
- Similarly, the color-coding of the alarm state for services links is displayed only if the option to display the alarm state for services links and link status are selected; these options are *not* selected by default.
- The node link data and alarm states for services links are automatically refreshed in the network monitoring topology only if the options to automatically refresh the topology is selected; this option is *not* selected by default.

The links on a node can also be rediscovered on demand manually by requesting for a rescan of a node.

RELATED DOCUMENTATION

Working with Topology | 887
Viewing the Node List | 809

Working with Topology

IN THIS SECTION

- Using the Search Option to View Nodes | 888
- Working with Topology Views | 889
- Viewing the Events and Alarms Associated with a Node | 890
- Viewing Alarms and Node Details | 891
- Viewing Nodes with Active Alarms | 893
- Managing Alarms Associated with Nodes | 893
- Viewing the Topology with Different Layouts | 893
- Automatic Refresh of the Topology | 894
- Viewing the Status of Node Links | 895
- Viewing the Alarm State of Services Links | 895
- Pinging a Node | 895

Viewing the Resource Graphs Associated with the Node | 896
Connecting to a Device by Using SSH | 897

On the Topology page in the Network Monitoring workspace, you can view nodes and node links, information about nodes and node status, and perform actions on nodes.

NOTE: On the Topology page, the term *node* refers to Junos Space nodes, FMPM nodes, or devices discovered by Junos Space Network Management Platform. The term *node link* refers to the link between the nodes.

Clicking a node or a node link highlights the node or node link. You can view the management IP address, name, and status for any node in the topology by hovering over the node, and the type of link, the name, the link bandwidth, and the endpoints by hovering over a node link. When you select a node or node link on the topology, the node or node link is highlighted. You can select multiple nodes by holding down the Ctrl key and selecting the nodes. You can use the zoom slider to zoom in and zoom out of the selected topology view. You can also use the semantic zoom-level functionality on the topology to display nodes one or more hops away from the selected nodes.

This topic contains the following sections:

Using the Search Option to View Nodes

You can use the Search option to search for and add nodes that you want to view in the topology. By default, no nodes are displayed in the topology and a warning message is displayed explaining how to add nodes to the topology.

Do one or more of the following:

- Enter **Nodes** in the **Search** field to select nodes from the list of all available nodes in the network topology.
- Enter **Category** in the **Search** field to select nodes by device category (Routers, Switches, Security Devices, and so forth).

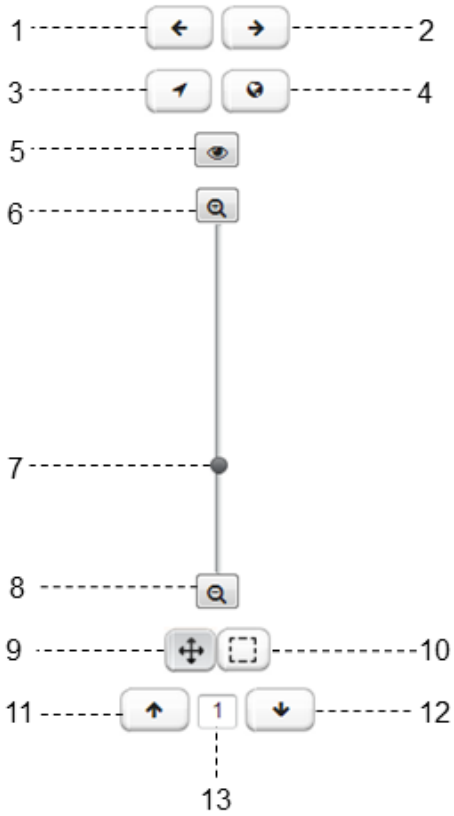
  NOTE:
  - Categories can be collapsed and expanded.
  - To display all nodes in the topology, select the Monitor_SNMP category.

- Enter the name of a specific device in the **Search** field to display a specific device.

Working with Topology Views

You can use the GUI controls, shown in Figure 47 and described in Table 115 to control the display of the nodes on the Topology page.

Figure 47: Topology View GUI Controls



1–**Click to go back** button	8–**Zoom slider**
2–**Click to go forward** button	9–**Pan** button
3–**Center on selection** button	10–**Selection** button
4–**Show entire map** button	11–**Expand semantic zoom** button
5–**Toggle highlight focus nodes** button	12–**Collapse semantic zoom** button
6–**Zoom in** button	13–**Number of connected hops from the node in focus**
7–**Zoom out** button	

Table 115: Topology Options

Option	Description
Click to go back button	View the previous topology view history.
Click to go forward button	View the more recent topology view history, after viewing the past history.
Center on selection button	Display the selected nodes in the center of the topology view.
Show entire map button	Display all the (filtered) nodes in the topology view.
Toggle highlight focus nodes button	When you add a node to focus, nodes connected to the focus node might also be displayed. When you click the **Toggle highlight focus nodes** button, only focus node icons are highlighted, and icons are dimmed for non-focus nodes that are connected to the focus nodes.
Zoom in button	Click to zoom in to the topology
Zoom slider	Move the slider up to zoom in or down to zoom out.
Zoom out button	Click to zoom out to the topology
Pan Tool button	Select on a node to reposition in topology view, or select between nodes (in white space) to pan all nodes in the topology view (up, down, left, or right) as a single image. To disable the Pan Tool function, click the **Selection Tool** button.
Selection Tool button	Perform operations on individual nodes (add node to focus, ping node, view node information, view events/alarms, and so forth). To disable the Selection Tool function, click the **Pan Tool** button.
Expand Semantic Zoom Level/Collapse Semantic Zoom Level	Expand or collapse the semantic zoom level by using the Up arrow key to increase the hop count or the Down arrow key to decrease the hop count. For example, select a hop count of 2 to display the network nodes two hops away from the focus nodes. **NOTE:** The topology view displays a line to show connections to nodes that are one or more hops away from a focus node.

Viewing the Events and Alarms Associated with a Node

In the **Topology** page, you can view the events and alarms associated with a node.

Do the following

1. Select **Network Monitoring** > **Topology**.

2. Right-click the node whose alarm associations you want to view and select **Events/Alarms**. Alternatively, you can also select the node and from the **Device** menu select **Events/Alarms** to view the events and alarms associated with the node.

   The events associated with the node are displayed in the **Events** tab in the **Events & Alarms** page (popup). For more information, see the "Viewing and Managing Events" on page 833 topic.

3. (Optional) To view the alarms associated with the node, select the **Alarms** tab in the **Events & Alarms** page.

   To view a specified number of events or alarms per page, select the required number from the list next to the **Results** field.

   By default, the number of items listed per page is 20. You can select the number of events or alarms you want to view per page from the **Show** list. You can choose to view 10, 20, 50, 100, 250, 500, or 1000 events or alarms.

   > **NOTE:** The number of events or alarms selected is set as user preference and the selected number of events or alarms are listed beginning from the next login.

   For more information, see the "Viewing and Managing Alarms" on page 844 topic.

Viewing Alarms and Node Details

To view details for a category of nodes or selected nodes:

1. Select **Network Monitoring** > **Topology**.

2. From the topology view, select a category of nodes or click the nodes you want to view.
   - To view alarm details for a category of nodes or selected nodes, select the **Alarms** tab towards the bottom of the page.

     The following alarm details are displayed:

     - ID—Alarm ID.
     - Severity—Severity of the alarm (Critical, Major, Minor, Warning, Normal, or Cleared).
     - Node—Name of the node.
     - UEI—The Unique Event Identifier (UEI), which is assigned to each event, including those generated by traps.
     - Count—Shows the number of events that were reduced to a single alarm row.

- Last Event Time—The most recent date and time when the alarm occurred.
- Log Message—The log message associated with the alarm.

- To view node details for the category of nodes or the selected nodes, select the **Nodes** tab.

  The following details are displayed for each node:

  - ID—Unique network monitoring ID associated with the node
  - Label—Name of the node
  - Creation Time—Date and time at which the node was added for network monitoring
  - Last Capabilities Scan—Date and time at which the capability scan was last performed
  - Primary Interface—Primary interface for the node in network monitoring
  - sysContact—Contact information, obtained by querying the node
  - sysDescription—Description of the node, obtained by querying the node
  - sysLocation—Location of the node
  - Foreign Source—Indicates that the node is a device managed by Junos Space Platform (**Space**) or that the node is a Junos Space or FMPM node (**Fabric**)
  - Foreign ID—Indicates the device ID in Junos Space Platform. The node ID from network monitoring is mapped to the device ID from Junos Space Platform

3. To view in-depth information about a node, right-click on the node and select **Node Info**.

   The Node Info page is displayed with the following information about the events and alarms associated with the node:

   - Availability
   - General Status
   - Node interfaces (IP interfaces and physical interfaces)
   - Surveillance Category Memberships
   - Notification (Outstanding/Acknowledged)
   - Recent events
   - Recent outages

   NOTE: The Node Info page provides an option to manually rediscover links on demand. Click the **Rescan** hyperlink and on the subsequent page click **Rescan**. You are taken back to the Node Info page; the topology is updated after approximately 1 minute.

Viewing Nodes with Active Alarms

To view nodes with active alarms:

1. Select **Network Monitoring** > **Topology**.

2. Use the Search option to select the nodes you want to check for active alarms.

   In the topology view, the color of the node icon indicates the highest severity alarm associated with the node. In addition, the node icon displays a number that indicates the count of outstanding alarms and notices associated with that node.

   > **NOTE:** A node with an active alarm of "Major" severity displays a red icon.

Managing Alarms Associated with Nodes

To acknowledge, unacknowledge, escalate, or clear the alarms associated with a node:

1. Select **Network Monitoring** > **Topology**.

2. From the topology page, select the nodes for which you want to manage alarms.

3. Select the **Alarms** tab.

4. Select the check box to the left of the alarm ID for each alarm listing you want to manage, or click **Select All** to manage all the listed alarms.

5. Select the action (Acknowledge, Unacknowledge, Escalate, or Clear) that you want to perform on the selected alarms.

6. Select **Submit** to complete the action.

Viewing the Topology with Different Layouts

To view the topology with different layouts:

1. Select **Network Monitoring** > **Topology**.

2. Select the **View** menu and then select the appropriate layout.

   By default, the topology is displayed in the FR layout.

You can view the topology using the following layouts:

- Circle Layout
- D3 Layout
- FR Layout
- Manual Layout
- Real Ultimate Layout

Automatic Refresh of the Topology

By default, the topology is not automatically refreshed.

To initiate an automatic refresh of the topology:

1. On the **View** menu of the Topology page (**Network Monitoring** > **Topology**), select the **Automatic Refresh** check box.

   The **View** menu is closed and you are taken back to the Topology page. The topology is automatically refreshed every 60 seconds.

If there are changes to the status of nodes, node links, and logical entities, these changes are displayed in the topology automatically.

Viewing the Status of Node Links

By default, the topology does not display the status of the node links.

To display the status of the node links in the topology:

1. On the **View** menu of the Topology page (**Network Monitoring** > **Topology**), select the **Link Status** check box.

   The **View** menu is closed and you are taken back to the Topology page. The topology now displays the status of the node links:

   - Green indicates that the link is up.
   - Red indicates that the link is down.

   > **NOTE:** If the Link Status check box is not selected, then the links are displayed in gray.

Viewing the Alarm State of Services Links

By default, the topology does not display the current alarm state of the services links within the topology.

To display the alarm state of the services links in the topology:

1. On the **View** menu of the Topology page (**Network Monitoring** > **Topology**), select the **NCS Link Status** check box. (NCS stands for Network Communication Services.)

   The **View** menu is closed and you are taken back to the Topology page. The topology now displays the alarm state of the services links:

   - Green indicates that the services link is up and that no service-impacted alarm was found.
   - Red indicates that the service status is down and that a service-impacted alarm is found for that service.

   > **NOTE:**
   > - If the Link Status check box is not selected, then the links are displayed in gray.
   > - If the NCS Link Status check box is cleared, then the link color is not changed automatically (dynamically) on the Topology page. If the NCS Link Status check box is selected, the color of the link changes automatically and dynamically based on the related alarms.
   > - When you mouse over a link, a tooltip displays the service information including the service status.

Pinging a Node

To ping a node:

1. Select **Network Monitoring** > **Topology**.

2. Right-click the node you want to ping and select **Ping** from the menu. Alternatively, you can also select the node and from the **Device** menu select **Resource Graphs** to view the resource graphs associated with the node.

   The Ping dialog box is displayed

3. In the **Number of Requests** field, enter the number of ECHO requests to be sent.

4. In the **Time-Out (seconds)** field, enter the number of seconds after which the ping request should time out.

5. From the **Packet Size** drop-down menu, select the size (in bytes) of the ping packet.

6. (Optional) Select the **Use Numerical Node Names** check box if you want the IP address to be displayed and not the hostname.

7. Click **Ping**.

   The node is pinged with the specified values and the results of the ping request is displayed on the lower part of the Ping page.

Viewing the Resource Graphs Associated with the Node

On the Topology page, you can view the resource graphs associated with a node.

Do the following:

1. Select **Network Monitoring** > **Topology**.

2. Right-click the node whose resource graphs you want to view and select **Resource Graphs**. Alternatively, you can also select the node and from the **Device** menu select **Resource Graphs** to view the resource graphs associated with the node.

   The node resources for which you can view graphs are displayed in the **Resource Graphs** page.

3. Select the resources for which you want to view the graphs and click **Graph Selection**.

> **NOTE:** You can also use the **Select All** and **Graph All** options to view the resource graphs for all node resources.

The resource graphs that you selected are displayed on the subsequent page. For more information, see the *Viewing Resource Graphs* section in the "Viewing Reports" on page 876 topic.

Connecting to a Device by Using SSH

On the **Topology** page (**Network Monitoring > Topology**), you can connect to one or more devices using SSH. You can also connect to the same device one or more times; a new SSH window is created for each connection.

> **NOTE:** The following is applicable irrespective of the type of authentication configured (credential-based or key-based) in Junos Space Platform:
>
> - If the option to allow users to automatically log in is configured, then users can automatically log in without providing a username and password. (You can configure the option to allow users to automatically log in to devices on the **Device** page (**Administration > Applications > Modify Application Settings > Device**). For more information, see the "Modifying Junos Space Network Management Platform Settings" on page 1346 topic.)
> - If the option to allow users to automatically log in is not configured, then, you are prompted to enter a username and password.
> - When you connect to a device by using SSH, Junos Space Platform validates the device fingerprint against the fingerprint stored in the database. If the fingerprints are the same, then Junos Space Platform allows you to connect to the device. If the fingerprints are not the same, then the behavior depends on the state of the **Manually Resolve Fingerprint Conflict** check box on the Modify Application Settings (Modify Network Management Platform Settings) page in the Administration workspace (**Administration** > **Applications** > ***Network Management Platform*** > **Modify Application Setting**).
>   - If the check box is selected, an error message is displayed indicating that there is a device fingerprint mismatch and the connection is dropped. The conflicted fingerprint value is updated in the database and the device's authentication status is marked **Fingerprint Conflict**. You must resolve the fingerprint conflict manually in order to connect to the device by using SSH. For more information, see "Acknowledging SSH Fingerprints from Devices" on page 295.
>   - If the check box is cleared, Junos Space Platform updates the new fingerprint in the database and allows a connection to the device; the device's authentication status is changed to **Credential Based – Unverified** or **Key Based – Unverified**.

To connect to a device by using SSH:

1. Select the device to which you want to connect.

   NOTE: You can connect only to devices and not to Junos Space nodes.

2. Right-click the device and select **SSH to Device**.

   - If the authentication is successful, the shell (CLI) for the device is displayed on a new page. The shell prompt is in the **root@*identifier*%** format, where *identifier* is a hostname of the node.

     CAUTION: Some browser plug-ins can cause undesirable behavior in open SSH windows; disabling such plug-ins might resolve the issue. For example, if the Firebug plug-in is activated within an SSH window opened in Firefox, the window cannot be restored, resized, or maximized and the console area remains fixed; disabling the Firebug plug-in resolves this issue.

   - If the authentication is not successful, the shell displays a message that the authentication has failed.

3. (Optional) After you have finished, type **exit** at the CLI prompt to close the session.

   A message is displayed indicating that the session is closed.

4. (Optional) Click the **Close** button on the browser page or tab to close the page.

NOTE: If you do not disconnect the session, the session is automatically disconnected by Junos Space in the following cases:

- When the user logs out
- When the user is logged out due to inactivity
- When the authentication is changed to certificate mode
- When the user is disabled or deleted
- When the user's session is terminated

RELATED DOCUMENTATION

Network Monitoring Topology Overview | 885
Network Monitoring Workspace Overview | 799
Resynchronizing Nodes in Network Monitoring | 813
Viewing the Node List | 809

Network Monitoring Topology Discovery Methods Supported by Junos Space Network Management Platform

Table 116 lists the topology discovery methods for the Juniper Networks devices supported in Junos Space Network Management Platform. For more information, see "Network Monitoring Topology Overview" on page 885.

Table 116: Topology Discovery Methods Supported for Network Monitoring

Product Series	Topology Discovery Methods
ACX Series	IS-IS, LLDP, OSPF
BX Series	OSPF
EX Series	Bridge Discovery Protocol, IS-IS, LLDP, OSPF
Firefly	IS-IS, LLDP, OSPF
J Series	IS-IS, LLDP, OSPF
LN Series	OSPF
M Series	IS-IS, OSPF
MX Series	IS-IS, LLDP, OSPF
PTX Series	IS-IS, OSPF
QFX Series	Bridge Discovery Protocol, IS-IS, OSPF
SRX Series	IS-IS, LLDP, OSPF
T Series	IS-IS, OSPF

RELATED DOCUMENTATION

Working with Topology | 887

CHAPTER 53

Network Monitoring Administration

IN THIS CHAPTER

- Configuring Network Monitoring System Settings | 901
- Updating Network Monitoring After Upgrading the Junos Space Network Management Platform | 904
- Configuring SNMP Community Names by IP | 912
- Configuring SNMP Data Collection per Interface | 913
- Managing Thresholds | 913
- Compiling SNMP MIBs | 918
- Managing SNMP Collections | 924
- Managing SNMPv3 Trap Configuration | 926
- Managing Data Collection Groups | 929
- Managing and Unmanaging Interfaces and Services | 933
- Starting, Stopping, and Restarting Services | 933

Configuring Network Monitoring System Settings

IN THIS SECTION

- Network Monitoring System Information | 902
- Generating a Log File for Troubleshooting | 903
- Changing the Notification Status | 903

You can view the network monitoring configuration and the system configuration on which network monitoring is running and generate network monitoring log reports for troubleshooting purposes.

This topic contains the following tasks:

Network Monitoring System Information

Select **Network Monitoring > Admin > System Information** to view the network monitoring configuration and the system configuration on which network monitoring is running.

The network monitoring Configuration section of the page lists the following information:

- Version
- Home Directory
- RRD store by Group—true or false
- Web-Application Logfiles—location
- Reports directory—location
- Jetty http host
- Jetty http port—usually 8980
- Jetty https host
- Jetty https port

The System Configuration section of the page lists the following information:

- Server Time
- Client Time
- Java Version
- Java Virtual Machine
- Operating System
- Servlet Container
- User Agent

Generating a Log File for Troubleshooting

To generate a log report for troubleshooting purposes:

1. Select one or more of the following plugins that you want to enable for reporting purposes:
   - Java: Java and JVM information
   - OS: Kernel, OS, and Distribution
   - Network monitoring: network monitoring core information, version, or basic configuration
   - TopEvent: Top 20 most reported events
   - Threads: Java thread dump (full output only)
   - Top: Output of the 'top' command (full output only)
   - lsof: Output of the 'lsof' command
   - Configuration: Append all network monitoring configuration files (full output only)
   - Logs:network monitoring log files (full output only)
2. Select the report type (text or zip file) to be generated.
3. Select **Submit Query**
4. You can view or save the file:
   - To view the report file, click **Open** from the File Download dialog box.
   - To save the report, click **Save** from the File Download dialog box.

Changing the Notification Status

Notifications are sent out only if the **Notification Status** is **On**. This is a system wide setting. The default setting is **Off**. After you change the setting, click **Update**.

To change the notification status:

1. In the **Notification Status** field, select **On** or **Off**.
2. Click **Update**.

   The notification status is changed and the page is reloaded.

RELATED DOCUMENTATION

Network Monitoring Workspace Overview | 799
Viewing the Node List | 809
Viewing Managed Devices | 194
Resynchronizing Nodes in Network Monitoring | 813
Searching for Nodes or Nodes with Asset Information | 816
Viewing, Configuring, and Searching for Notifications | 865

Updating Network Monitoring After Upgrading the Junos Space Network Management Platform

IN THIS SECTION

- Overview | 904
- Step 1: Monitoring the Software Install Status Window for File Conflicts | 904
- Step 2: Identifying Files with Conflicts | 906
- Step 3: Merging Files with Conflicts | 908
- Step 4: Verifying the Manual Merge Status of Configuration Files | 909
- Step 5: Final Steps After Upgrading Network Monitoring | 910

Overview

After upgrading the Junos Space Network Management Platform, the Network Monitoring configuration files might not contain the configuration file changes for the latest version. During the Junos Space Network Management upgrade process, the Software Install Status window displays a message if there are any configuration files in conflict. You can also access the **/var/log/install.log** file to view any files that have conflicts. To manually merge files that contain conflicts, you must perform all of the following steps. When the upgrade process encounters no files in conflict, the files are auto-merged and you do not need to perform the following steps.

Step 1: Monitoring the Software Install Status Window for File Conflicts

Check for the following message in the Software Install Status window during the upgrade of the Junos Space Network Management Platform:

```
WARNING: Conflict observed during OpenNMS git-merge so please merge the changes
manually:
Please go to folder /opt/opennms/etc, and merge the *.old.bak files to current
running files.
```

When logged in from the Junos Space Network Management Platform command-line interface (CLI), you can also check for file conflicts from the **/var/log/install.log** file. The following example message from the **install.log** file shows three files with conflicts that you will need to manually merge to resolve:

```
opennms-post.pl 62: Error while running git merge
opennms-auto-upgrade/pristine: merge -Xpatience
-Xignore-space-change -Xignore-all-space -Xrenormalize
opennms-auto-upgrade/pristine:
command returned error: 1 at /usr/lib/perl5/site_perl/5.8.8/Error.pm line 343.

opennms-post.pl 63: The following files are in conflict:

opennms-post.pl 65: eventconf.xml

opennms-post.pl 65: events/ncs-component.events.xml

opennms-post.pl 65: linkd-configuration.xml
```

NOTE: If no files with conflicts are found during the upgrade process, the files are automatically merged, and you do not need to perform any additional steps. Otherwise, you must complete each of the following steps.

Step 2: Identifying Files with Conflicts

If you discovered one or more files with conflicts during the previous step, perform the following steps to identify the files with conflicts:

1. Log in to the virtual IP (VIP) fabric node.

2. Stop the Network Monitoring service from the Junos Space Network Management Platform user interface:

   a. Select **Network Management Platform > Administration > Applications**.

      The Applications page appears.

   b. Right-click **Network Management Platform** and click **Manage Services**. (Alternatively, you can select **Network Management Platform** and click **Manage Services** from the Actions menu.)

      The Manage Services page is displayed.

   c. Select the **Network Monitoring** service and click the **Stop Service** icon.

      The **Confirm Stop SNMP Agent** dialog box is displayed.

   d. Click **Yes**.

      A status dialog box with a message indicating that the service has stopped is displayed.

   e. Click **OK**.

      A dialog box is displayed confirming that the service has successfully stopped.

   f. Click **OK**.

      You are taken to the Manage Services page.

3. From the Junos Space Network Management Platform CLI, check the status of the Network Monitoring service by executing the following command:

```
# su - opennms -c '/sbin/service opennms status'
```

Junos Space displays the message **opennms is stopped**.

4. To re-merge the Network Monitoring configuration files:

   a. From the Junos Space CLI, execute the following command:

   ```
   # /opt/opennms/bin/config-tools/conflict-remerge.pl
   ```

   Junos Space displays output similar to the following:

   ```
   conflict-remerge.pl 19: Resetting tree to
   'opennms-auto-upgrade/tags/runtime/pre-1.13.0-0.20131227.1'
   ```

   b. Navigate to the **/opt/opennms/etc** directory and execute the following command:

   ```
   # git status
   ```

   Most of the files are auto-merged. If any files remain, the status of each file in conflict is displayed under the section “Unmerged paths” and is marked "both modified", as shown in the following example:

   ```
   Unmerged paths:
   # (use "git add/rm ..." as appropriate to mark resolution)
   # both modified: eventconf.xml
   # both modified: events/ncs-component.events.xml
   # both modified: linkd-configuration.xml
   ```

   For each remaining conflicted file (listed under Unmerged paths) changes that were made to the file are identified with the opening statement "**<<<<<< HEAD**" and closing statement "**>>>>>>> opennms-auto-upgrade/pristine**". For example, in the **ncs-component.events.xml** file shown above, the file changes are marked as follows:

   ```
   <<<<<<< HEAD
   ```

```
<alarm-data-reduction
key="%uei%:%parm[componentType]%:%parm[componentForeignSource]%
:%parm[componentForeignId]%" alarm-type="2"

clear-

key="uei.opennms.org/internal/ncs/componentImpacted:%parm[componentType]%
:%parm[componentForeignSource]%:%parm[componentForeignId]%"
auto-clean="false"/>

======

<alarm-data-reduction-

key="%uei%:%parm[componentType]%:%parm[componentForeignSource]%
:%parm[componentForeignId]%:%parm[nodeid]%" alarm-type="2"

clear-

ei.opennms.org/internal/ncs/componentImpacted:%parm[componentType]%
:%parm[componentForeignSource]%:%parm[componentFo

]%:%parm[nodeid]%"

auto-clean="false"/>

>>>>>>> opennms-auto-upgrade/pristine
```

Step 3: Merging Files with Conflicts

After identifying the files with conflicts, you must perform the following steps to manually merge each of the files and resolve all conflicts:

1. From a VI editor, open the file with conflicts.

2. Search for the statement "HEAD".

3. Identify the differences between the two configurations which are contained between the lines **<<<<< HEAD** and **>>>>> opennms-auto-upgrade/pristine**.

   a. The configuration for the file *before* the upgrade is contained between the lines **<<<<< HEAD** and **========**.

b. The configuration for the file *after* the upgrade is contained between the lines **========** and **>>>>> opennms-auto-upgrade/pristine**.

4. Save the configuration of the file *after* the upgrade, and then update it with any user-modified values from the configuration file *before* the upgrade.

5. After manually merging configuration file changes, remove each of the following lines from the file:

```
<<<<<<< HEAD

============

>>>>>>> opennms-auto-upgrade/pristine
```

6. Save the configuration file.

7. Repeat steps 2 through 6 for each configuration file with conflicts until all file conflicts in all files are merged.

   After all the file conflicts are merged, there should be no occurrence of the following lines:

```
<<<<<<< HEAD

============

>>>>>>> opennms-auto-upgrade/pristine
```

Step 4: Verifying the Manual Merge Status of Configuration Files

From the Junos Space CLI, execute the following commands to verify that the configuration file changes are merged correctly:

```
/opt/opennms/bin/config-tools/conflict-resolve.pl

git status
```

If the file changes were merged correctly, Junos Space displays the following message:

```
nothing to commit (working directory clean)
```

Step 5: Final Steps After Upgrading Network Monitoring

Perform the following steps after upgrading Network Monitoring:

1. Update permissions of the **/opt/opennms** directory to **774**:

```
# chmod -R 774 /opt/opennms
```

2. Run the following command to change the ownership of the **/opt/opennms** directory to **opennms:space**:

```
#chown -R opennms:space /opt/opennms
```

3. Verify that the **opennms.conf** file includes the line **RUNAS="opennms"**:

```
# more opennms.conf

START_TIMEOUT=0

ADDITIONAL_MANAGER_OPTIONS="-Djava.io.tmpdir=/opt/opennms/tmp -d64
-XX:MaxPermSize=512m -

XX:HeapDumpPath=/var/opennms/java_pid <pid>.hprof
-XX:+HeapDumpOnOutOfMemoryError -XX:+PrintGCTimeStamps -XX:+PrintGCDetails"

JAVA_HEAP_SIZE=2048

RUNAS="opennms" #######Verify that this line exists
```

4. The password of the user “postgres” in the **opennms-datasources.xml** file will be empty. Set the password to **postgres**:

```
<jdbc-data-source name="opennms-admin"
```

```
database-name="template1"

class-name="org.postgresql.Driver"

url="jdbc:postgresql://localhost:5432/template1"

user-name="postgres"

password="postgres" /> #######Password is set here
```

5. Start the Network Monitoring service from the Junos Space user interface:

   a. Select **Network Management Platform** > **Administration** > **Applications**.

      The Applications page appears.

   b. Right-click Network Management Platform and select **Manage Services** or select **Network Management Platform** and click **Manage Services** from the Actions menu.

      The Manage Services page appears.

   c. Select the **Network Monitoring** service and click the Start Service icon.

      The Confirm Start message appears.

   d. Click **YES**.

6. If your fabric is running in a multi-node setup, execute the following command to verify that all the modified configuration files are synchronized across the standby node:

```
# /opt/opennms/contrib/failover/scripts/sync.sh
```

RELATED DOCUMENTATION

Upgrading Junos Space Network Management Platform | 1378

Starting, Stopping, and Restarting Services | 933

Configuring SNMP Community Names by IP

This task enables you to configure SNMP community names by IP address. You also need to configure the community string used in SNMP data collection. The network monitoring functionality is shipped with the *public* community string. If you have set a different *read* community on your devices, this is where you must enter it.

In this procedure, you enter a specific IP address and community string, or a range of IP addresses and a community string, and other SNMP parameters. The network monitoring functionality optimizes this list, so enter the most generic addresses first (that is, the largest range) and the specific IP addresses last, because if a range is added that includes a specific IP address, the community name for the specific address is changed to be that of the range. For devices that have already been discovered and have an event stating that data collection has failed because the community name changed, you might need to update the SNMP information on the interface page for that device (by selecting the Update SNMP link) for these changes to take effect.

To configure SNMP using an IP address:

1. Select **Network Monitoring > Admin > Configure SNMP Community Names by IP**, and enter in the First IP Address field either a single IP address, or the first address of a range.

2. If you are not entering a range of IP addresses, leave the Last IP Address field blank, otherwise enter the last IP address of the range.

3. In the Community String field, enter the community string you use for your devices. The default is *public*.

4. (Optional) Enter a timeout in the Timeout field.

5. Select the appropriate version from the Version list.

6. (Optional) Enter the number of retries in the Retries field.

7. (Optional) Enter the port number in the Port field.

8. Click **Submit**. The system displays a message telling you whether network monitoring needs to be restarted for the configuration to take effect.

RELATED DOCUMENTATION

Configuring SNMP Data Collection per Interface | 913

Configuring SNMP Data Collection per Interface

For each different SNMP collection scheme, there is a parameter called SNMP Storage Flag. If this value is set to primary, then only values pertaining to the node as a whole or the primary SNMP interface are stored in the system. If this value is set to all, then all interfaces for which values are collected are stored. If this parameter is set to select, then the interfaces for which data is stored can be selected. By default, only information from primary and secondary SNMP interfaces are stored.

You can choose other non-IP interfaces on a node if you have set up the SNMP collection.

To manage SNMP data collection for each interface:

1. Select **Network Monitoring > Admin > Configure SNMP Data Collection per Interface**.

   The Manage SNMP Data Collection per Interface page appears.

2. Select the node for which you want to manage data collection.

   The Choose SNMP Interfaces for Data Collection page appears listing all known interfaces.

3. Select the appropriate value for the interface in the Collect column.

   Primary and secondary interfaces are always selected for data collection.

RELATED DOCUMENTATION

Managing SNMP Collections | **924**

Managing Thresholds

IN THIS SECTION

- Creating Thresholds | **914**
- Modifying Thresholds | **916**
- Deleting Thresholds | **917**

Thresholds allow you to define triggers against any data retrieved by the SNMP collector, and generate events, notifications, and alarms from those triggers. You can add, remove, and modify thresholds.

Creating Thresholds

To create a threshold:

1. Select **Network Monitoring > Admin > Manage Thresholds**.

   The Threshold Configuration page appears and lists the threshold groups that are configured on the system.

2. To create a new threshold for a threshold group, select **Edit** next to the threshold group.

   The Edit group page appears.

3. Select **Create New Threshold**.

   The Edit threshold page appears.

4. To configure the threshold, specify appropriate values for the following threshold fields:
   - Type—Specify high, low, relativeChange, absoluteChange, or rearmingAbsoluteChange.
   - Datasource–Specify a name for the datasource.
   - Datasource type—Specify a datasource type from the list.
   - Datasource label—Specify a type from the list.
   - Value—Use depends on the type of threshold.
   - Re-arm— Specify the name of a custom UEI to send into the events system when this threshold is re-armed. If left blank, it defaults to the standard thresholds UEIs.
   - Trigger–Specify the number of times the threshold must be exceeded in a row before the threshold is triggered.

     NOTE: A trigger is not used for relativeChange thresholds.

   - Description—(Optional) A description used to identify the purpose of the threshold.
   - Triggered UEI— A custom UEI to send into the events system when the threshold is triggered. If a UEI is not specified, it defaults to the standard thresholds UEIs in the format *uei.opennms.org/<category>/<name>*.
   - Re-armed UEI—A custom UEI to send into the events system when this threshold is re-armed. If left blank, it defaults to the standard thresholds UEIs.

5. Select **Save** to create the threshold in Junos Space Network Management Platform.

6. (Optional) To configure a resource filter for a threshold:

   a. Configure a filter operator to define the logical function to apply for the threshold filter to determine whether or not to apply the threshold. An OR operator specifies that if the resource matches any of the filters, the threshold is processed. An AND operator specifies that the threshold is processed only when a resource match all the filters.

   b. Specify a field name for the filter operator to define the logical function to apply for the threshold filter to determine whether or not to apply the threshold.

   c. Specify the mathematical expression with data source names that is evaluated and compared to the threshold values.

   d. Select the **Add** action to add the filter to a threshold.

To create an expression-based threshold:

1. Select **Network Monitoring > Admin > Manage Thresholds**.

   The Threshold Configuration page appears and lists the threshold groups that are configured on the system.

2. To create a new threshold for a threshold group, select **Edit** next to the threshold group.

   The Edit group page appears.

3. Select **Create New Expression-based Threshold**.

   The Edit expression threshold page appears.

4. To configure the threshold, specify appropriate values for the following expression threshold fields:

   - Type—Specify high, low, relativeChange, absoluteChange, or rearmingAbsoluteChange.
   - Expression–Specify a mathematical expression that includes the datasource names which are evaluated and compared to the threshold values.
   - Datasource type—Specify a datasource type from the list.
   - Datasource label—Specify a type from the list.
   - Value—Use depends on the type of threshold.
   - Re-arm— Specify the name of a custom UEI to send into the events system when this threshold is re-armed. If left blank, it defaults to the standard thresholds UEIs.

- Trigger–Specify the number of times the threshold must be exceeded in a row before the threshold is triggered.

  NOTE: A trigger is not used for relativeChange thresholds.

- Description—(Optional) A description used to identify the purpose of the threshold.
- Triggered UEI— A custom UEI to send into the events system when the threshold is triggered. If a UEI is not specified, it defaults to the standard thresholds UEIs in the format *uei.opennms.org/<category>/<name>*.
- Re-armed UEI—A custom UEI to send into the events system when this threshold is re-armed. If left blank, it defaults to the standard thresholds UEIs.

5. Select **Save** to create the expression threshold in Junos Space Network Management Platform.

6. (Optional) To configure a resource filter for an expression threshold:

   a. Configure a filter operator to define the logical function to apply for the expression threshold filter to determine whether or not to apply the expression threshold. An OR operator specifies that if the resource matches any of the filters, the expression threshold is processed. An AND operator specifies that the expression threshold is processed only when a resource match all the filters.

   b. Specify a field name for the filter to define the logical function to apply for the threshold filter to determine whether or not to apply the threshold.

   c. Specify the mathematical expression with data source names that are evaluated and compared to the threshold values.

   d. Select the **Add** action to add the filter to an expression threshold.

Modifying Thresholds

To modify an existing threshold in a threshold group:

1. Select **Network Monitoring > Admin > Manage Thresholds**.

   The Threshold Configuration page appears and lists the threshold groups that are configured on the system.

2. To create a new threshold for a threshold group, select **Edit** next to the threshold group.

   The Edit group page appears.

3. To modify an existing threshold, select the **Edit** option that appears to the right of the threshold you want to update.

   The Edit Threshold page appears and displays the threshold fields.

4. Modify the threshold fields you want to update.

5. Click **Save** to update the threshold.

6. (Optional) To add a resource filter for the threshold:

   a. Specify a filter operator to define the logical function to apply for the threshold filter to determine whether or not to apply the threshold. An OR operator specifies that if the resource matches any of the filters, the threshold is processed. An AND operator specifies that the threshold is processed only when a resource match all the filters.

   b. Specify a field name for the filter to define the logical function to apply for the threshold filter to determine whether or not to apply the threshold.

   c. Specify the mathematical expression with data source names that are evaluated and compared to the threshold values.

   d. Select the **Add** action to add the filter to the threshold.

Deleting Thresholds

To delete a threshold:

1. Select **Network Monitoring > Admin > Manage Thresholds**.

   The Threshold Configuration page appears and lists the threshold groups that are configured on the system.

2. To delete a threshold from a threshold group, select **Edit** next to the threshold group.

   The Edit group page appears.

3. To delete an existing threshold, select **Delete**.

RELATED DOCUMENTATION

Network Monitoring Workspace Overview | 799

Compiling SNMP MIBs

IN THIS SECTION

- Uploading MIBs | 918
- Compiling MIBs | 919
- Viewing MIBs | 919
- Deleting MIBs | 920
- Clearing MIB Console Logs | 920
- Generating Event Configuration | 920
- Generating a Data Collection Configuration | 922

Uploading MIBs

To upload a MIB file:

1. Select **Network Monitoring > Admin**.

   The Admin page is displayed.

2. Select **SNMP MIB Compiler** in the Operations section of the Admin page.

3. Click **Upload MIB**.

4. Browse and upload the MIB file from the appropriate location where the MIB file is stored.

   The MIB file you have uploaded is displayed in the pending node of the MIB tree. You can now view and compile this MIB file.

   NOTE: The filename must be the same as the MIB being processed.

Compiling MIBs

Before you compile a MIB file, ensure that you have uploaded the MIB file. The MIB file should be displayed in the pending node of the MIB tree for you to be able to compile the MIB file.

To compile a MIB file:

1. Select **Network Monitoring > Admin**.

   The Admin page is displayed.

2. Select **SNMP MIB Compiler** in the Operations section of the Admin page.

3. From the pending node of MIB tree, right-click the MIB file you want to compile and select **Compile MIB**.

   You can view the results of the MIB compilation in the MIB Console section of Admin page. If the MIB file is compiled successfully, you will receive a log entry “MIB parsed successfully”. If the MIB file cannot be complied, you will receive an error message.

   If a MIB file is compiled successfully, the MIB file will be moved from the pending node to the compiled node in the MIB tree.

Viewing MIBs

You can view MIB files in the compiled state or in the pending state.

To view a MIB file:

1. Select **Network Monitoring > Admin**.

   The Admin page is displayed.

2. Select **SNMP MIB Compiler** in the Operations section of the Admin page.

3. Right-click the MIB file you want to view and select **View MIB**.

   The View MIB pop-up window displays the MIB file. Use the scroll bar to view the contents of the MIB file.

Deleting MIBs

You can delete MIB files in the compiled state or in the pending state.

To delete a MIB file:

1. Select **Network Monitoring > Admin**.

   The Admin page is displayed.

2. Select **SNMP MIB Compiler** in the Operations section of the Admin page.

3. Right-click the MIB file you want to delete and select **Delete MIB**.

4. Click **Yes**.

Clearing MIB Console Logs

MIB console displays the logs related to MIB file upload and MIB file compilation.

To clear the MIB console logs:

1. Select **Network Monitoring > Admin**.

   The Admin page is displayed.

2. Select **SNMP MIB Compiler** in the Operations section of the Admin page.

3. Click **Clear Log** in the MIB console section.

Generating Event Configuration

You can generate event configuration from traps after you have compiled the MIB files.

To generate an event configuration:

1. Select **Network Monitoring > Admin**.

   The Admin page is displayed.

2. Select **SNMP MIB Compiler** in the Operations section of the Admin page.

3. From the complied node in the MIB tree, right-click a MIB file and select **Generate Events**.

4. In the Generate Events pop-up window, click **Continue**.

You can edit the UEI base if needed. The Events window now displays the events that are currently part of the MIB file. You can choose to save this events XML file as is, edit this events XML file, or add new events to this file.

5. To save the events file as is, click **Save Events File**.

6. To add new events:
   a. Click **Add Event**.

      Enter the new event details.
   b. In the **Event UEI** field, enter a unique event identifier.
   c. In the **Event Label** field, enter a label for the new event.
   d. In the **Description** field, enter a description for the new event.
   e. In the **Log Message** field, enter a log message for the new event.
   f. From the **Destination** drop down menu, select an appropriate option.
   g. From the **Severity** drop down menu, select an appropriate option.
   h. In the **Reduction Key** field, enter appropriate text.
   i. In the **Clear Key** field, enter appropriate text.
   j. From the **Alarm Type** drop down menu, select an appropriate option.
   k. In the **Operator Instructions** field, enter instructions for the operator if required.
   l. Click **Add** next to the **Mask Elements** table to add new element names and element values.
   m. Click **Add** next to the **Mask Varbinds** table to add new varbind numbers and varbind values.
   n. Click **Add** next to the **Varbind Decodes** table to add new parameter IDs and decode values.
   o. Click **Save**.
   p. Click **Yes**.
7. To edit the current events XML file:
   a. Select the event you want to edit.
   b. Scroll down to the bottom of the window and select **Edit**.

      You can now edit all the parameters of this event.
8. After you have added new events or modified the events, click **Save Events File**.

NOTE: Once an event file is saved, reference is added to **eventconf.xml** and an event configuration reload operation is performed.

Generating a Data Collection Configuration

You can generate a data collection configuration for performance metrics after you have compiled the MIB files.

To generate a data collection configuration:

1. Select **Network Monitoring > Admin**.

   The Admin page is displayed.

2. Select **SNMP MIB Compiler** in the Operations section of the Admin page.

3. From the complied node in the MIB tree, right-click a MIB file and select **Generate Data Collection**.

   The Data Collection window is displayed. You can save the data collection XML file as is or add new resource types, MIB groups, and system definitions to this data collection XML. You can also modify the existing resource types, MIB groups, and system definitions before saving the data collection XML.

4. In the **Data Collection Group Name** field, modify the group name if required.

5. To save the data collection XML as is, click **Save Data Collection File**.

6. To add a new resource type to the data collection XML:
   a. Select the **Resource Types** column in the Data Collection window.
   b. Click **Add Resource Type**.

      Enter the resource type details.
   c. In the **Resource Type Name** field, enter a name for the resource.
   d. In the **Resource Type Label** field, enter a label for the resource.
   e. In the **Resource Label** field, enter appropriate text.
   f. From the **Class Name** drop down menu, select the appropriate class name for storage strategy.
   g. Click **Add** next to the Storage Strategy table to add new parameters.
   h. From the **Class Name** drop down menu, select the appropriate class name for persist selector strategy.

i. Click **Add** next to the Persist Selector Strategy table to add new parameters.

j. Click **Save**.

7. To edit an existing resource type in the data collection XML:
   a. Select the **Resource Types** column in the Data Collection window.
   b. Select the resource type you want to edit.
   c. Scroll down to the bottom of the window and select **Edit**.

      You can now edit all the parameters of this resource type.
8. To add a new MIB group to the data collection XML:
   a. Select the **MIB Groups** column in the Data Collection window.
   b. Click **Add Group**.

      Enter the MIB group details.
   c. In the **Group Name** field, enter a name for the MIB group.
   d. From the **ifType Filter** drop down menu, select the appropriate option.
   e. Click **Add** next to the **MIB Objects** table to add the OID, instance, alias, and type for the MIB objects.
   f. Click **Save**.
9. To edit an existing MIB group in the data collection XML:
   a. Select the **MIB Groups** column in the Data Collection window.
   b. Select the MIB group you want to edit.
   c. Scroll down to the bottom of the window and select **Edit**.

      You can now edit all the parameters of this MIB group.
10. To add a new system definition to the data collection XML:
    a. Select the **System Definitions** column in the Data Collection window.
    b. Click **System Definition**.

       Enter the system definition details.
    c. In the **Group Name** field, enter a name for the system definition.
    d. Select the appropriate buttons next to the System OID/Mask field.
    e. Select the MIB group you want to associate this system definition to, and click **Add Group**.

       The MIB group is displayed in the MIB Groups table.
    f. Click **Save**.
11. To edit an existing system definition in the data collection XML:
    a. Select the **System Definitions** column in the Data Collection window.

b. Select the system definition you want to edit.

c. Scroll down to the bottom of the window and select **Edit**.

You can now edit all the parameters of this system definition.

NOTE: Update the datacollection-config.xml to include the group created into an SNMP collection when you have generated a data collection.

RELATED DOCUMENTATION

Network Monitoring Workspace Overview | 799

Managing SNMP Collections

IN THIS SECTION

Adding a New SNMP Collection | 924
Modifying an SNMP Collection | 925

Adding a New SNMP Collection

To add a new SNMP collection:

1. Select **Network Monitoring > Admin**.

   The Admin page is displayed.

2. Select **Manage SNMP Collections and Data Collection Groups** in the Operations section of the Admin page.

3. Select the **SNMP Collections** tab.

4. Click **Add SNMP Collection**.

5. In the **SNMP Collection Name** field, enter a name for the SNMP collection.
6. From the **SNMP Storage Flag** drop down menu, select an appropriate value.
7. Click **Add** next to the RRA list table and add consolidation function, XFF, steps, and rows for RRD.
8. Click **Add** next to the Include Collections table and add the include types and values.
9. Click **Save**.

Modifying an SNMP Collection

To modify an SNMP collection:

1. Select **Network Monitoring > Admin**.

   The Admin page is displayed.

2. Select **Manage SNMP Collections and Data Collection Groups** in the Operations section of the Admin page.
3. Select the **SNMP Collections** tab.
4. Click **Refresh SNMP Collection**.
5. Select the appropriate SNMP collection name.
6. Scroll down to the bottom of the window and click **Edit**.

   You can now edit all the parameters of this SNMP collection.

7. Click **Save**.

RELATED DOCUMENTATION

Network Monitoring Workspace Overview | 799

Managing SNMPv3 Trap Configuration

From Junos Space Platform Release 17.1R1 onward, you can modify the SNMPv3 trap configuration from the Junos Space Platform GUI. The Junos Space Network Management Platform stores the SNMPv3 trap configuration in the **/opt/opennms/etc/trapd-configuration.xml** file.

When a device is discovered using SNMPv3, Junos Space Platform sends the latest SNMPv3 trap configuration, which is the first item in the **trapd-configuration.xml** file, to the newly-discovered device. Modifications to SNMPv3 trap configuration trigger a restart of the OpenNMS and deployment of the latest configuration onto the devices.

The SNMPv3 trap configuration includes the username, security level, and authentication and privacy settings. Although you can configure multiple users, only the last modified user configuration is deployed onto the devices. The default username is *JunosSpace*. The security level for the *JunosSpace* user is by default set to *authPriv*.

> **NOTE:**
>
> After you upgrade Junos Space Platform to Release 17.1R1 or later, modify the SNMPv3 trap configuration from the Junos Space Platform UI or merge the old and new configuration as explained in "Updating Network Monitoring After Upgrading the Junos Space Network Management Platform" on page 904.

To modify the SNMPv3 trap configuration on the Junos Space Platform:

1. On the Junos Space Platform UI, select **Network Monitoring** > **Admin** > **SNMPv3 Trap Configuration**.

   The SNMPv3 Trap Configuration page appears.

2. In the **User Name** field, enter a unique username.

3. From the **Security Level** list, select one of the following values:

   authPriv —Enables both authentication and privacy settings. if you select this, you need to specify both authentication and privacy settings.

   authNoPriv —Enables authentication without privacy settings. if you select this, you need to specify the authentication settings. The privacy settings remain disabled in the Platform UI.

   NoAuthNoPriv —Disables both authentication and privacy settings. If you select this, you cannot configure authentication or privacy settings. The authentication and privacy settings remain disabled in the Platform UI.

4. If you selected **authPriv** or **authNoPriv** from the **Security Level** list, configure the following authentication settings:

   Authentication Type —Select **MD5** or **SHA**.

   Authentication Password —Type the authentication password for the user.

   Confirm Authentication Password —Retype the authentication password to confirm.

   > **NOTE:** These fields remain disabled if you selected **NoAuthNoPriv** from the **Security Level** list.

5. If you selected **authPriv** from the **Security Level** list, configure the following privacy settings:

   Privacy Type —Select **AES** or **DES**.

   Privacy Password —Type the privacy password for the user.

   Confirm Privacy Password —Retype the privacy password to confirm.

   > **NOTE:** These fields remain disabled if you selected **authNoPriv** or **NoAuthNoPriv** from the **Security Level** list.

6. To submit the changes, click **OK**. Alternatively, to discard the changes and close the page, click **Cancel**.

   If you click **OK**, Junos Space Platform displays the following message: **Modifying SNMPv3 Trap Configuration. This action will restart OpenNMS and deploy the updated SNMP configuration to the managed devices**. To submit the changes, click **Yes**. After you click **Yes**, OpenNMS restarts and Junos Space Platform deploys the modified configuration onto the managed devices.

   If you click **Yes**, the job ID is displayed. You can click the job ID to view the job details and status.

   > **NOTE:** If you click **Yes** without modifying the SNMPv3 trap configuration, Junos Space Platform displays the following message: **No configuration changed. Please Change SNMPv3 Configuration Before Submit**.

   You can click **No** to go back to the SNMPv3 Trap Configuration page.

Device-side Configuration for SNMPv3 Traps

For Junos Space Platform to be able to manage SNMPv3 traps on the managed devices, you must complete the following device-side configuration:

NOTE: Words in *Italics* in the following examples indicate variables. You may need to replace that with the corresponding values used in your configuration.

```
snmp {
    v3 {
        usm {
            local-engine {
                user "JunosSpace" {
                    authentication-md5 {
                        authentication-key authentication-key
                    }
                    privacy-des {
                        privacy-key privacy-key
                    }
                }
            }
        }
        target-address TA_SPACE {
            address ip-address;
            tag-list TAG_SPACE;
            target-parameters TP_SPACE;
        }
        target-parameters TP_SPACE {
            parameters {
                message-processing-model v3;
                security-model usm;
                security-level privacy;
                security-name "JunosSpace";
            }
            notify-filter SPACE_TRAP_FILTER;
        }
        notify SPACE_TRAPS {
            type trap;
            tag TAG_SPACE;
        }
        notify-filter SPACE_TRAP_FILTER {
            oid .1 include;
```

```
        }
      }
    }
```

The corresponding **set** commands are:

```
set snmp v3 usm local-engine user JunosSpace authentication-md5 authentication-key authentication-key
set snmp v3 usm local-engine user JunosSpace privacy-des privacy-key privacy-key
set snmp v3 target-address TA_SPACE address ip-address
set snmp v3 target-address TA_SPACE tag-list TAG_SPACE
set snmp v3 target-address TA_SPACE target-parameters TP_SPACE
set snmp v3 target-parameters TP_SPACE parameters message-processing-model v3
set snmp v3 target-parameters TP_SPACE parameters security-model usm
set snmp v3 target-parameters TP_SPACE parameters security-level privacy
set snmp v3 target-parameters TP_SPACE parameters security-name JunosSpace
set snmp v3 target-parameters TP_SPACE notify-filter SPACE_TRAP_FILTER
set snmp v3 notify SPACE_TRAPS type trap
set snmp v3 notify SPACE_TRAPS tag TAG_SPACE
set snmp v3 notify-filter SPACE_TRAP_FILTER oid .1 include
```

Managing Data Collection Groups

IN THIS SECTION

- Adding New Data Collection Files | **930**
- Deleting Data Collection Files | **930**
- Modifying Data Collection Files | **931**

Adding New Data Collection Files

To add a new data collection file:

1. Select **Network Monitoring > Admin**.

   The Admin page is displayed.

2. Select **Manage SNMP Collections and Data Collection Groups** in the Operations section of the Admin page.

3. Select the **Data Collection Groups** tab.

4. Click **Add New Data Collection File**.

   The New Data Collection Group pop-up window is displayed.

5. In the **Group Name** field, enter a name for data collection group.

6. Click **Continue** to add and configure the data collection file.

Deleting Data Collection Files

To delete a data collection file:

1. Select **Network Monitoring > Admin**.

   The Admin page is displayed.

2. Select **Manage SNMP Collections and Data Collection Groups** in the Operations section of the Admin page.

3. Select the **Data Collection Groups** tab.

4. From the Select Data Collection Group File drop-down menu, select the data collection file you want to remove.

5. Click **Remove Selected Data Collection File**.

6. Click **Yes.**

Modifying Data Collection Files

You can edit the resource types, MIB groups, or system definitions in the data collection file or add new resource types, MIB groups, or system definitions to this file.

1. Select **Network Monitoring > Admin**.

   The Admin page is displayed.

2. Select **Manage SNMP Collections and Data Collection Groups** in the Operations section of the Admin page.

3. Select the **Data Collection Groups** tab.

4. From the **Select Data Collection Group File** drop down menu, select the data collection file you want to modify.

5. To add a new resource type to the data collection file:
   a. Select the **Resource Types** column in the Data Collection window.
   b. Click **Add Resource Type**.

      Enter the resource type details.
   c. In the **Resource Type Name** field, enter a name for the resource.
   d. In the **Resource Type Label** field, enter a label for the resource.
   e. In the **Resource Label** field, enter appropriate text.
   f. From the **Class Name** drop down menu, select the appropriate class name for storage strategy.
   g. Click **Add** next to the Storage Strategy table to add new parameters.
   h. From the Class Name drop-down menu, select the appropriate class name for the persist selector strategy.
   i. Click **Add** next to the Persist Selector Strategy table to add new parameters.
   j. Click **Save**.
6. To edit an existing resource type in the data collection file:
   a. Select the **Resource Types** column in the Data Collection window.
   b. Select the resource type you want to edit.
   c. Scroll down to the bottom of the window and select **Edit**.

      You can now edit all the parameters of this resource type.
7. To add a new MIB group to the data collection file:

a. Select the **MIB Groups** column in the Data Collection window.

b. Click **Add Group**.

   Enter the MIB group details.

c. In the **Group Name** field, enter a name for the MIB group.

d. From the **ifType Filter** drop down menu, select the appropriate option.

e. Click **Add** next to the MIB Objects table to add the OID, instance, alias, and type for the MIB objects.

f. Click **Save**.

8. To edit an existing MIB group in the data collection file:

   a. Select the **MIB Groups** column in the Data Collection window.

   b. Select the MIB group you want to edit.

   c. Scroll down to the bottom of the window and select **Edit**.

      You can now edit all the parameters of this MIB group.

9. To add a new system definition to the data collection file:

   a. Select the **System Definitions** column in the Data Collection window.

   b. Click **System Definition**.

      Enter the system definition details.

   c. In the **Group Name** field, enter a name for the system definition.

   d. Select the appropriate radio buttons next to the System OID/Mask field.

   e. Select the MIB group to which you want to associate this system definition, and click **Add Group**.

      The MIB group is now displayed in the MIB Groups table.

   f. Click **Save**.

10. To edit an existing system definition in the data collection file:

    a. Select the **System Definitions** column in the Data Collection window.

    b. Select the system definition you want to edit.

    c. Scroll down to the bottom of the window and select **Edit**.

       You can now edit all the parameters of this system definition.

11. When you have made the necessary changes, select **Save Data Collection File**.

RELATED DOCUMENTATION

Network Monitoring Workspace Overview | 799

Managing and Unmanaging Interfaces and Services

To manage a service, you must manage its interface. The Manage and Unmanage Interfaces and Services page enables you to manage not only interfaces, but also the combination of node, interface, and service. The tables on this page display the latter, with the Status column indicating if the interface or service is managed or not.

Managing an interface or service means that the network monitoring functionality performs tests on this interface or service. If you want to explicitly enable or disable testing, you can set that up here. A typical case is if a webserver is listening on both an internal and an external interface. If you manage the service on both interfaces, you will get two notifications if it fails. If you want only one notification, unmanage the service on one of the interfaces.

Select **Network Monitoring > Admin > Manage and Unmanage Interfaces and Services** to manage or unmanage your node, interface, and service combinations.

To change the status, you have these choices: **Apply Changes**, **Cancel**, **Select All**, **Unselect All**, or **Reset**.

Starting, Stopping, and Restarting Services

This topic describes how to start, stop, and restart Network Monitoring (that is, the network monitoring services). Currently, Network Monitoring is the only service that can be managed this way.

Service management operations—start, stop, restart—are applied on all the nodes that run the service.

The service management actions generate audit log entries.

The Super Administrator and System Administrator predefined roles have the permissions to manage services; the corresponding action is Manage Services. If a user does not have a role that includes this action, the Manage Services option is not available.

The following table describes the consequences of performing these three actions:

Table 117: Starting, Stopping, and Restarting Network Monitoring

Action	Consequences
Stop	Network Monitoring service is stopped on all nodes.
	Even if VIP failover is performed, service remains stopped on all nodes.
	The synchronization of network monitoring data is disabled.
	Even after adding a new node, the network monitoring service remains stopped.
	Rebooting Junos Space Network Management Platform does not restart a service.
Start, **Restart**	Network Monitoring service starts only on the VIP node.
	All the devices displayed on the Devices page are discovered by the network monitoring functionality. The SNMP trap targets are correct.
	All the users displayed on the Users page are added to network monitoring.
	E-mail and remote server settings are added to network monitoring.
	All Junos Space nodes are monitored by the network monitoring functionality.
	The service continues to be operational even if Junos Space Network Management Platform is rebooted.
Start, Stop, Restart when no service is selected	An error message is displayed: No service selected.

NOTE: The following firewall ports should be closed on stopping the network monitoring service:

- UDP
  - 162
  - 514
  - 5813
- TCP
- 5813
- 18980

> **NOTE:** Any devices added while the Network Monitoring service is stopped must be manually resynchronized from the Network Monitoring workspace after the service is restarted.

To start, stop, or restart network monitoring services:

1. Select **Administration** > **Applications**.

   The Applications inventory page appears.

2. Select **Network Management Platform** and select **Manage Services** from the Actions menu.

   The Manage Services page appears, showing the names of the services that can be managed this way (currently, Network Monitoring is the only item on this list), and the Start, Stop, and Restart buttons, as well as a table displaying the following information:

Column Heading	Content
Service Name	Name of service that can be started, stopped or restarted
Running Version	Version of the service that is currently running
Status	Current status: Enabled or Disabled

3. Select **Network Monitoring** from the list, and select the relevant button for a currently enabled service: **Start Service**, **Restart Service**, or **Stop Service**.

   One of four messages appears:

   - If you select a service that is currently running, then select **Stop Service**, you will receive this message:

     ```
     Confirm Stop Service: Do you really want to stop the service?
     ```

   - If you select a service that has been disabled, then select **Restart Service**, you will receive this message:

     ```
     Warning: Sorry, cannot proceed with the request, as the Service is not
     in Enabled state.
     ```

   - If you select a service that has been disabled, then select **Start Service**, you will receive this message:

```
Warning: Sorry, Network Monitoring cannot be started once it is stopped.
```

- If you select a service that has been disabled, then select **Stop Service**, you will receive this message:

```
Warning: Sorry, cannot proceed with the request, as the Service is already
in Disabled state.
```

4. In all cases, you can click only **OK**.

   You first receive a message indicating that the relevant action is being performed. This is followed by a second status message indicating whether the operation you performed was successful or not.

5. Click **OK** to confirm.

   The Manage Services page reappears, displaying the changed status of the selected service.

RELATED DOCUMENTATION

- Managing Junos Space Applications Overview | **1328**
- Managing and Unmanaging Interfaces and Services | **933**
- Network Monitoring Workspace Overview | **799**
- Junos Space Audit Logs Overview | **1115**
- Role-Based Access Control Overview | **995**

8

PART

Configuration Files

Overview | **938**

Managing Configuration Files | **942**

CHAPTER 54

Overview

IN THIS CHAPTER

- Managing Configuration Files Overview | 938
- Viewing Configuration File Statistics | 940

Managing Configuration Files Overview

Configuration files in Junos Space Network Management Platform are created when device configuration data from managed devices are backed up to the Junos Space Platform database for the first time. A separate configuration file is created in the database for each managed device. Each time the configuration of a device changes, a new version of the configuration file is created on the device, which can then be backed up to the Junos Space Platform database or to a remote server at a fixed time, or at a set recurrence interval periodically.

Centralized configuration file management enables you to maintain multiple versions of your device configuration files in Junos Space Platform. This helps you recover device configuration files in case of a system failure and maintain consistent configuration across multiple devices.

> **NOTE:** Version management for configuration files in Junos Space Platform is independent of configuration file versioning on devices. Each **commit** command on a device creates a new version of the configuration file on the device, but no more than 49 versions can be stored on a device. However, Junos Space Platform allows you to store more than 49 versions of a configuration file on the Junos Space server.

The configuration files workspace helps you manage the following configuration files:

- Running configuration—The configuration file currently in effect on the device. The running configuration file is labeled Version 0.
- Candidate configuration—The new, not yet committed, configuration file that will become the running configuration.

- Backup configuration—The configuration file for recovery or rollback purposes. When you execute a **commit** command, a backup configuration file is created and the oldest backup file (Version 49) is deleted from the device. The most recent backup configuration file is labeled Version 1.

The following is a potential workflow for an individual file or device in this workspace:

1. Back up the device configuration file and thus bring the device's running configuration under Junos Space Platform management.
2. Edit a copy of the backup configuration file to create a candidate configuration file.
3. Verify edits by comparing the initial backup version of the configuration file with the edited version.
4. Restore the candidate configuration file to the device.
5. Export the initial backup version to a zip file.

Over a period of time, the number of device configuration files that are backed up in Junos Space Platform database increases. Accumulation of configuration files in the database could increase the overhead to the database and adversely affect the overall performance of the server. You can purge the device configuration files that are older than the latest 2 versions of the configuration files that are backed up.

To purge the older device configuration files, use the **/var/www/cgi-bin/cleanUpDevConfigBackup.sh** script.

On the Junos Space Platform UI, you can view stored configuration files on the **Configuration Files** > **Config Files Management** page. For information about the roles that you need to be assigned to perform various tasks related to configuration files, see "Predefined Roles Overview" on page 999.

On the Config Files Management page, you can perform the following actions:

- Backing Up Configuration Files on page 943
- Viewing Configuration Files on page 948
- Restoring Configuration Files on page 958
- Comparing Configuration Files on page 953
- Modifying Configuration Files on page 955
- Exporting Configuration Files on page 960
- Deleting Configuration Files on page 962

RELATED DOCUMENTATION

Viewing Configuration File Statistics | 940

Viewing Configuration File Statistics

The Configuration Files statistics page displays two bar charts: the **Configuration file count by device family** bar chart and the **Devices with most frequently revised configuration files** bar chart. You can use these charts to help manage device configuration files in Junos Space Network Management Platform.

The **Configuration file count by device family** chart helps you view the number of different device configurations in each device family and the **Devices with most frequently revised configuration files** chart lets you view the number of times a device configuration changed.

To view the **Configuration file count by device family** chart:

1. On the Junos Space Network Management Platform UI, select **Configuration Files**.

   The Configuration Files statistics page appears, displaying the **Configuration file count by device family** and the **Devices with most frequently revised configuration files** bar charts. On the Configuration file count by device family chart, the x-axis represents the device family and the y-axis represents the number of configuration files. Mouse over a device family bar on the Configuration file count by device family chart to view a tooltip showing the number of configuration files for the device family.

2. (Optional) Click a device-family bar on the Configuration file count by device family chart.

   The Config Files Management page appears, displaying the configuration files and devices that are part of the selected device family. You can double-click any configuration file to view its details.

To view the **Devices with most frequently revised configuration files** chart:

1. On the Junos Space Network Management Platform UI, select **Configuration Files**.

   The Configuration Files statistics page appears, displaying the **Configuration file count by device family** and the **Devices with most frequently revised configuration files** bar charts. Mouse over a device bar on the Devices with most frequently revised configuration files chart to view a tooltip showing the number of configuration file versions for the device.

2. (Optional) Click a device bar on the Devices with most frequently revised configuration files chart.

   The Config Files Management page appears, displaying the configuration file for the selected device. You can double-click the configuration file to view different versions of the file.

You can return to the Configuration Files statistics page by clicking **Configuration Files** on the left pane of the Junos Space UI or by clicking **Configuration Files** on the breadcrumbs at the top of the page.

RELATED DOCUMENTATION

Backing Up Configuration Files | 943

Managing Configuration Files Overview | 938

Tags Overview | 1506

CHAPTER 55

Managing Configuration Files

IN THIS CHAPTER

- Backing Up Configuration Files | **943**
- Viewing Configuration Files | **948**
- Comparing Configuration Files | **953**
- Modifying Configuration Files | **955**
- Restoring Configuration Files | **958**
- Exporting Configuration Files | **960**
- Deleting Configuration Files | **962**

Backing Up Configuration Files

Junos Space Network Management Platform enables you to back up device configuration information by importing the configuration file from a device and storing it in Junos Space Platform or on a remote server. You can use this backup file to recover device configuration in case of a system failure and also to maintain consistent configuration across multiple devices. Backing up your device configuration files is therefore a prerequisite for configuration file management.

> **NOTE:** Only devices that have been previously discovered by Junos Space Platform can have their configuration files backed up.

The backup function skips over devices that cannot be accessed by the Junos Space server. On the Job Management page, the state of a configuration file backup job shows up as Failed in the case of skipped over devices.

The backup function checks for differences between the configuration file on the device and the configuration backup file stored in Junos Space Platform before creating a new version of the configuration file. If no changes are detected, the device is skipped over. However, the status is shown as Success on the Job Management page for this backup configuration job.

> **NOTE:** The backup function checks for differences between the configuration file on the device and the configuration backup file stored in Junos Space Platform. In case the device configuration has not changed, but you edit its configuration file in Junos Space Platform and then back up the configuration from the device, a new version is created. The first backup file is Version 1, the edited configuration file is Version 2, and the second backup file is Version 3.

When you back up a configuration file, an audit log entry is automatically generated. From the audit log entry, you can identify the user who initiated the backup operation, the IP address from which this task was initiated, and so on.

> **NOTE:** In the case of an SRX Series device with logical system (LSYS), configuration file backup is supported only on the root device.

To back up configuration files from one or more devices to Junos Space Platform:

1. On the Junos Space Platform UI, select **Configuration Files** > **Config Files Management**.

   The Config Files Management page appears.

2. Click the Backup Configuration Files icon.

   The Backup Configuration Files page appears, displaying the following information for all the devices managed by Junos Space Platform:

   - Host Name: Name of the device whose configuration file you are backing up
   - Device Alias: Value of the Device Alias custom label for the device
   - Domain: Domain to which the device belongs
   - IP Address: IP address of the device
   - Platform: Device platform
   - Serial Number: Serial number of the device
   - Software Version: Operating system firmware version running on the device

   Because the table displays one device (record) per row, a single page might not be sufficient to list all your devices.

   The left side of the status bar at the bottom of the page shows which page is currently displayed and the total number of pages of records. It also provides controls for navigating from page to page and refreshing them. The right side of the status bar indicates the number of records currently displayed and the total number of records.

3. From the table, select the devices whose configurations you want to back up, by using one of the following selection modes—manually, on the basis of tags, or on the basis of domains. These options are mutually exclusive. If you select one, the others are disabled.

   NOTE:
   - By default, the **Select by Device** option button is selected and the complete list of devices is displayed.
   - If you want to back up the configuration of all devices, select the **Select All across Pages** check box.

   To select devices manually:

   a. Click the **Select by Device** option and select the devices whose configurations you want to back up.

      The Select Devices status bar shows the total number of devices that you selected, dynamically updating as you select.

b. (Optional) To back up all the devices, select the check box in the column header next to the **Host Name** column.

To select devices on the basis of tags:

a. Click the **Select by Tags** option.

   The Select by tags list is activated.

b. Click the arrow on the **Select by tags** list.

   A list of tags defined for devices in Junos Space Platform appears, displaying two categories of tags—Public and Private.

   > **NOTE:** If no tags are displayed, then it means that none of the devices are associated with any tag. You need to tag the devices first on the Device Management page before you can use the **Select by Tags** option. For more information about tagging, see "Tagging an Object" on page 1526.

c. To select tags, perform one of the following actions:

   - Select the check boxes next to the tag names to select the tags and click **OK**.
   - To search for a specific tag, enter the first few letters of the tag name in the **Select by Tags** field to the left of the **OK** button. If a match is found, a suggestion is made; you can select it and click **OK**.

   The total number of devices associated with the selected tags appears just above the device display table. For example, if there are six devices associated with the selected tags, then **6 items selected** is displayed.

   The selected tags appear next to the **Tags Selected** label. An [X] icon appears after each tag name. Click the [X] icon to clear any tag from the list. The device count decrements accordingly.

To select devices on the basis of domains:

a. Click the **Select by Domains** option.

   The Select by domains list is activated.

b. Click the arrow on the **Select by domains** list.

   The list of domains appears. Only the domains that you have access to are available for selection.

c. Select the check boxes next to the domain names to select the desired domains and click **OK**.

The total number of devices associated with the selected domains appears just above the device display table.

The selected domains appear next to the **Domain(s) Selected** label. An [X] icon appears after each domain name. Click the [X] icon to clear any domain from the list. The device count decrements accordingly.

4. (Optional) To export the backed-up configuration file to a remote server, select the **Export backup to a remote scp server** check box and provide the following details:

   - **IP Address**: Enter the IP address of the remote server.
   - **Port**: Enter the port number. If you do not specify the port number, the default port, 22, is used.
   - **Directory**: Enter the directory path for backup.
   - **Username**: Enter your username.
   - You can select the authentication mode for backing up configuration file to SCP server from Junos Space Network Management Release 17.1R1 onward.
     - To use the password mode, in the **Password** field, enter the password that you use to access the SCP server. By default, the **Password** mode is selected.
     - To use a key generated from Junos Space Platform, click **Space Key**. Click the **Download Space Key** link to download the key.

       NOTE: Alternatively, you can download the Space Key by selecting **Administration** > **Fabric** and clicking the Manage Space SSH Key icon.

       After downloading the Space Key, log in to the SCP server and append the contents of the downloaded key file to the **~/.ssh/authorized_keys** file.

     - To use a custom private key, click **Custom Key**.

       (Optional) In the **Passphrase** field, enter the passphrase created when you generated the private key.

       Next to the **Private Key** field, click the Browse button to upload the private key.

   - **Fingerprint**: (Optional) Enter the fingerprint of the remote server.

   Junos Space Platform uses Secure Copy Protocol to back up the configuration file to the specified folder in the remote server. The name of the file is in the following format:

   <device_name>_<device_ip>_<version>_<timestamp>.conf.gz

Here, **device_name** is the name of the device, **device_ip** is the IP address of the device, **version** is the configuration file version and **timestamp** is the date and time the configuration file is backed up.

5. (Optional) To schedule a time for backup of configuration files, select the **Schedule at a later time** check box, and use the calendar icon and the drop-down list, to specify the date and the time respectively.

   If you do not select the **Schedule at a Later Time** check box, the configuration files are backed up as soon as you click the **Backup** button on the Backup Config Files page.

   > **NOTE:** If a backup is already scheduled for later using password mode, in order to use Space Key or Custom Key, you must cancel the existing scheduled task and reschedule it using the authentication mode of your choice.
   >
   > If a backup is already scheduled for later using Custom Key and if the key has changed, you must cancel the existing scheduled task and reschedule it using the updated key.

6. (Optional) Schedule configuration files backup recurrence by selecting the **Repeat** check box.

   To set the recurrence:

   a. Specify the backup recurrence by setting the interval and the increment.

      The default recurrence interval is 1 hour.

   b. Select the **End Time** check box to specify when the recurrence must end.

      Indicate a date and time by using the date calendar and the time list. If you do not specify an end date and time, the backup operation recurs until you cancel the job manually.

   If recurrence is set and the **Export backup to a remote scp server** check box is selected, the configuration file is copied to the remote server at specified intervals.

   > **NOTE:** You can schedule the automatic export of backed-up configuration files to a remote Secure Copy Protocol (SCP) server only from Junos Space Network Management Platform Release 16.1R1 onward.

7. Click **Backup** on the Backup Configuration Files page.

   The Backup Configuration Files dialog box appears, displaying a message indicating that Junos Space Platform has successfully scheduled the backup of the selected configuration files.

8. Perform one of the following actions:

- Click the job ID in the Backup Configuration Files dialog box to view the status of the configuration file backup job from the Job Management page.

  To return to the Config Files Management page, click **Configuration Files** > **Config Files Management** on the task tree.

- Click **OK** in the Backup Configuration Files dialog box.

  The Config Files Management page reappears, displaying the backup files.

  For more information about viewing the backup configuration files, see "Viewing Configuration Files" on page 948.

For troubleshooting, see the **/var/log/jboss/servers/server1/server.log** file.

Release History Table

Release	Description
17.1R1	You can select the authentication mode for backing up configuration file to SCP server from Junos Space Network Management Release 17.1R1 onward.
16.1R1	You can schedule the automatic export of backed-up configuration files to a remote Secure Copy Protocol (SCP) server only from Junos Space Network Management Platform Release 16.1R1 onward.

RELATED DOCUMENTATION

Managing Configuration Files Overview | **938**

Deleting Configuration Files | **962**

Restoring Configuration Files | **958**

Comparing Configuration Files | **953**

Modifying Configuration Files | **955**

Exporting Configuration Files | **960**

Tagging an Object | **1526**.

Viewing Audit Logs | **1117**

Viewing Configuration Files

The Configuration Files workspace enables you to manage multiple versions of device configuration files in Junos Space Network Management Platform. You can view information about all configuration files

that are backed up in the Junos Space Platform database from the Config Files Management page. To view detailed information about a particular file, you can use the View Configuration File Details option.

To view configuration files:

1. On the Junos Space Platform UI, select **Configuration Files** > **Config Files Management**.

   The Config Files Management page appears, displaying information about configuration files in tabular format. The fields displayed on the Config Files Management page are described in Table 118.

   > **NOTE:** If a column is not displayed by default, click the down arrow next to a displayed column and select the column you want to view from the **Columns** list. You can also filter the records that are displayed, based on the data in all the columns except the Creation Date and Last Updated Date columns.

2. Select a configuration file entry and click the **View Configuration File Details** icon. You can also double-click a configuration file entry to view the details of that configuration file.

   The Config File Details dialog box appears. In addition to the fields displaying information about the configuration file, the Config File Details dialog box also displays the contents of the configuration file. By default, the contents of the latest version of the configuration file are displayed.

   The vertical and horizontal scroll bars help you view the configuration file. A configuration file usually has multiple pages. The status bar at the bottom displays the page that you are on and the total number of pages. It also contains paging controls and a Refresh icon. Use the **Show items** list to manage the number of lines of configuration that is displayed on a single page. By default, 50 lines are displayed. You can choose to display 200, 800, 3200, or 10,000 lines.

   This dialog box displays additional fields not displayed on the Config Files Management page. The fields are described in Table 118.

3. (Optional) To view the contents of an earlier version of the configuration file, click the arrow on the version drop-down list and select the version you want to view.

4. Click **Close** to return to the Config Files Management page.

Table 118: Config Files Management Page and Config File Details Dialog Box Field Descriptions

Field	Description	Location
Config File Name	Name of the configuration file. This is the device serial number with the **.conf** file extension.	Config Files Management page

Table 118: Config Files Management Page and Config File Details Dialog Box Field Descriptions *(continued)*

Field	Description	Location
Device Name	Name or IP address of the device whose configuration is backed up	Config Files Management page Config File Details dialog box
Device Alias	Value of the Device Alias custom label for the device. This field is empty if the Device Alias custom label is not added or no value is assigned to the Device Alias custom label for the device.	Config Files Management page
Latest ConfigFile Version	Version number of the latest backup of the configuration file	Config Files Management page
Creation Date	Date and time when version 1 of the configuration file is created in the Junos Space database. It corresponds to the time at which you back up a device configuration for the first time from the device. When you migrate from a previous release of Junos Space Platform to the current release, the creation date that is displayed for the various versions of the configuration files is the date on which those versions were created in the previous release of Junos Space Platform. For example, if you modified version 1 of the configuration file to version 2 on Dec 15 2012 7:28:46 PM IST in Junos Space Release 13.1 and migrated to Junos Space Release 13.3R1 in 2014, the creation date for version 2 is displayed as Dec 15 2012 7:28:46 PM IST instead of a date in 2014.	Config Files Management page

Table 118: Config Files Management Page and Config File Details Dialog Box Field Descriptions *(continued)*

Field	Description	Location
Last Updated Date	Date and time when the latest version of the configuration file is created in the Junos Space database. When you modify the device configuration, and back up the configuration file, a newer version of the configuration file is created in the Junos Space database.	Config Files Management page
Creation Time	Date and time when version 1 of the configuration file selected for viewing is created in the Junos Space database. This is the same as the Creation Date field on the Config Files Management page.	Config File Details dialog box
Version	Configuration file version selected for detailed viewing You can select the configuration file version whose contents you want to view by clicking the arrow to display the version list.	Config File Details dialog box
ConfigFile Content	Contents of the configuration file version selected for detailed viewing	Config File Details dialog box

Table 118: Config Files Management Page and Config File Details Dialog Box Field Descriptions *(continued)*

Field	Description	Location
Comments	Indicates whether the configuration file version is backed up from the device or is an edited version of a configuration file that was backed up earlier. For the initial backup file, the following comment is displayed: **This version of the Config file is imported from the device.** For an edited configuration file, the following comment is displayed: **This is an edited version of the configuration file version: *x***, where *x* represents the version of the configuration that you edited.	Config File Details dialog box

RELATED DOCUMENTATION

- Managing Configuration Files Overview | **938**
- Backing Up Configuration Files | **943**
- Exporting Configuration Files | **960**

Comparing Configuration Files

Junos Space Network Management Platform enables you to compare two device configuration files by using the Compare Configuration File Versions action. You can view entire device configuration files side by side to compare them, see the total number of differences, the date and time of the last commit operation, and the number of changes made.

You can compare device configuration files in any of the following ways:

- The configuration file of one device with the configuration file of another device. By default, the latest versions are compared.
- Two versions of the same configuration file. By default, the latest version and the previous version are compared.
- An earlier version of the configuration file of one device with a later version of the configuration file of another device

Comparing configuration files does not generate an audit log entry.

To compare device configuration files:

1. On the Junos Space Network Management Platform UI, select **Configuration Files > Config Files Management**.

   The Config Files Management page appears, displaying all the configuration files managed by Junos Space Platform.

2. On the Config Files Management page, select the configuration file that you want to compare.

3. Select **Compare Configuration File Versions** from the Actions menu.

   The Compare Config Files page appears.

4. For the source, select the source device from the **Source Device** list and a version of its configuration file from the **ConfigFile Version** list.

   The timestamp is displayed adjacent to the version number. It indicates the time at which this version of the configuration was backed up.

5. For the target, select the target device from the **Target Device** list and a version of its configuration file from the **ConfigFile Version** list.

   The timestamp is displayed adjacent to the version number. It indicates the time at which this version of the configuration was backed up.

6. Click **Compare**.

The View Diff page appears and displays the two selected configuration files side by side, with the device names and their versions in a dark gray bar underneath the legend at the top of the page.

The legend references the following:

- **Total diffs**—Black text indicates content that is common to both files.
- **Source**—Green text indicates content in the source file on the left that is not contained in the target file on the right.
- **Target**—Blue text indicates content in the target file on the right that is not contained in the source file on the left.
- **Changed**—Pink text indicates content that is changed.

The status bar shows the current page number and the total number of pages. It also provides controls for moving from page to page and for refreshing the display.

The date and time of the last commit operation is shown in pink.

> **NOTE:** When you compare files, each configuration parameter in one file or version is set side by side with the same parameter in the other. Therefore, you might see multiple pages of configuration for a single parameter in one file, whereas the same parameter in the other file might be only a few lines long.

7. (Optional) To locate differences in configuration, click **Prev Diff** or **Next Diff**.

8. (Optional) To export differences in the configuration to your local system, click **Export Diff**.

   A dialog box appears prompting you to save the zip file.

   a. Save the zip file to your computer. The filename is of the following format: ***source-hostname.VersionNumber_target-hostname.VersionNumber*.conf.zip**

   b. (Optional) Extract the zip file and open the extracted file by using a text editor.

      The file lists the differences in the configuration. The first two lines in the extracted file represent the device name, version number, and timestamp of the configuration files that were compared.

   When you export the configuration differences, an audit log entry is automatically generated.

9. Click **Close** at the bottom of the View Diff page to stop viewing the comparison.

   You are returned to the Compare Config Files page.

10. Click **Cancel** to exit the Compare Config Files page.

You are returned to the Config Files Management page.

RELATED DOCUMENTATION

- Backing Up Configuration Files | 943
- Managing Configuration Files Overview | 938
- Deleting Configuration Files | 962
- Restoring Configuration Files | 958
- Modifying Configuration Files | 955
- Exporting Configuration Files | 960

Modifying Configuration Files

Junos Space Network Management Platform allows you to modify device configuration files from the Configuration Files workspace. The **Modify Configuration File** action in the Configuration Files workspace enables advanced users to modify device configuration files stored in the Junos Space database.

> **NOTE:** When you edit a configuration file in the Configuration Files workspace, the configuration is not validated and a sanity check is not performed. For more information on validating device configuration, see "Reviewing and Deploying the Device Configuration" on page 327. To ensure that the configuration is validated and a sanity check is performed, use the Devices workspace to modify device configuration. For more information, see "Modifying the Configuration on the Device" on page 322.

When you edit a configuration file, an audit log entry is automatically generated (see "Viewing Audit Logs" on page 1117); however, unlike configuration files edited in the Devices workspace, files edited in the Configuration Files workspace are not saved as change requests; instead, they are saved as versions. The audit log entry records the name of the configuration file that was modified.

To edit a configuration file in the Configuration Files workspace:

1. On the Junos Space Platform UI, select **Configuration Files > Config Files Management**.

   The Config Files Management page appears.

2. On the Config Files Management page, select the device whose configuration you want to edit.

If no configuration files are displayed on the page, first back up the device configuration file. For more information about backing up device configuration, see "Backing Up Configuration Files" on page 943. You can then select the configuration file from the Config Files Management page.

3. Click the **Modify Configuration File** icon at the top of the Config Files Management page.

   The Edit Config File page appears. It displays the name of the device whose configuration you want to edit, the time at which the file was created, the version of the file with the timestamp (that is, when the configuration snapshot was created), and the contents of the file.

4. From the **Version** list, select a version to use as a baseline. By default, the latest version of the file is displayed.

   The timestamp is displayed adjacent to the version number. It indicates the time at which this version of the configuration was backed up.

   A version can be either a configuration backup file or an edited copy of the initial backup file. For more information about versioning, see "Backing Up Configuration Files" on page 943.

   The selected version appears in the text editor. The vertical and horizontal scroll bars help you view the configuration file. A configuration file usually has multiple pages. The status bar at the bottom displays the page that you are on and the total number of pages. It also contains paging controls and a Refresh icon. Use the **Show items** list to manage the number of lines of configuration that is displayed on a single page. By default, 50 lines are displayed. You can choose to display 200, 800, 3200, or 10,000 lines.

5. (Optional) To find a specific parameter, go through the file page by page. The browser's Search function does not work in the text editor.

6. Enter your changes.

   > **NOTE:** Do not click **Modify** until you have finished editing. Clicking **Modify** will create a new version of the configuration file.

7. (Optional) List the changes you have made (or any other information that you want to add) in the **Comments** field. You cannot add a comment unless you have made changes to the configuration. It is advisable to enter text in this field to distinguish the current version from a backup taken from the device itself.

8. After you have made all changes, click **Modify**.

   The Config Files Management page reappears, displaying the edited configuration file that is still selected.

> **NOTE:** Junos Space does not create a new version of the configuration file if you have not made any changes to the device configuration. That is, if you click Modify without making any changes to the device configuration, then Junos Space displays the following message: **Config file contents are same as the current version. To save as a latest version, please change the contents or select a previous version to be saved as the latest.**

Verify your changes by double-clicking the configuration file on the Config Files Management page.

The Config File Details dialog box appears, displaying the file in noneditable format. You can select the version from the **Version** list. By default, the latest edited version appears.

The pagination, Comments area, and controls are the same as they are in the text editor you used to make your changes.

If you want to view the differences between the recently modified version and a previous version, you can compare versions of the file. For more information about comparing device configuration files, see "Comparing Configuration Files" on page 953.

To deploy the edited configuration file on to a device, you must use the Restore Configuration File action. See "Restoring Configuration Files" on page 958 for more information.

RELATED DOCUMENTATION

- Managing Configuration Files Overview | **938**
- Deleting Configuration Files | **962**
- Exporting Configuration Files | **960**
- Backing Up Configuration Files | **943**
- Viewing Audit Logs | **1117**

Restoring Configuration Files

Using Junos Space Network Management Platform, you can save and restore the configuration of managed devices. The Restore Configuration Files action from the Configuration Files workspace enables you to deploy any version of the backup device configuration file to the device. You can also deploy an edited version of the configuration file to the device. Restoring a configuration file involves either merging the contents of the selected configuration file version on Junos Space Platform with the device's running configuration file or overriding the device's running configuration file with the selected version of the configuration backup file from Junos Space Platform.

When you restore a configuration file, an audit log entry is automatically generated.

To restore a device configuration file from Junos Space Platform to a device:

1. On the Junos Space Platform UI, select **Configuration Files** > **Config Files Management**.

   The Config Files Management page appears.

2. On the Config Files Management page, select the configuration file that you want to restore. (To restore all of them, select the check box next to the first column header.)

3. Select **Restore Configuration Files** from the Actions menu.

   The **Restore Config File(s)** dialog box appears, displaying the name of the selected file, the name of the device, the version that is to be restored to the device, and the type of restore. By default, the latest version of the configuration file is merged with the existing configuration on the device. If any of the columns is not displayed by default, click the down arrow next to any of the displayed columns and select the columns that you want to view from the **Columns** list.

4. Select the required version from the drop-down list that appears when you click next to the version number displayed in the **ConfigFile Version** column.

   The date and time at which the version of the configuration was backed up is displayed adjacent to the version number.

5. Select the type of restore from the list that appears when you click the term displayed in the **Type** column. You can opt to merge the contents of a configuration file on Junos Space Platform with the existing configuration file on the device or override the device's running configuration file with a candidate configuration file (a configuration file edited in the Configuration Files workspace) or a configuration backup file from Junos Space Platform.

6. (Optional) To restore the configuration file at a later time, select the **Schedule at a later time** check box and use the calendar icon and drop-down list, to specify the date and time respectively.

If you do not select the **Schedule at a Later Time** check box, the configuration file is restored as soon as you click **Restore** on the Restore Config File(s) dialog box.

7. Click **Restore** on the Restore Config File(s) dialog box.

   The Restore Configuration Files dialog box appears. The dialog box displays a message indicating that the restore action was successfully scheduled, and also displays a link to a job ID.

8. Click **OK** to return to the Config Files Management page or click the job ID link to view details of the restore job. If the restore action was successful, the Status column on the Job Management page shows success. If a device cannot be accessed, it is skipped over and the job status indicates a failure.

   To identify the reason for the failure of a restore job:

   a. Double-click the entry for the failed restore job.

      The Configuration File Management Job Status page appears.

   b. From the **Status** column on the Configuration File Management Job Status page, locate the job that has failed.

   c. For the failed job, click **View Results** in the **Description** column.

      The Job Description page appears, displaying the reason for the failure.

   d. Click **Close**.

      You are returned to the Configuration File Management Job Status page.

   e. Click the [X] icon at the top right of the Configuration File Management Job Status page to return to the Job Management page.

To verify that the configuration file is restored on the device, perform another backup operation and then compare versions (see "Comparing Configuration Files" on page 953).

RELATED DOCUMENTATION

- Managing Configuration Files Overview | **938**
- Deleting Configuration Files | **962**
- Comparing Configuration Files | **953**
- Modifying Configuration Files | **955**
- Exporting Configuration Files | **960**

Backing Up Configuration Files | 943
Viewing Audit Logs | 1117

Exporting Configuration Files

With Junos Space Network Management Platform, you can export configuration files from the Junos Space server. The Export action enables you to save and compress one or more configuration files into a zip folder on your local computer. You can later view or compare the downloaded configuration files offline.

> **NOTE:** Your browser security settings must be set to allow downloads. If the browser interrupts the download with a warning and you try to restart the download by refreshing the browser, the export operation is stopped and the zip folder removed.

When you export a configuration file, an audit log entry is automatically generated.

To export a configuration file into a zip folder on your local computer:

1. On the Junos Space Network Management Platform UI, select **Configuration Files > Config Files Management**.

   The Config Files Management page appears.

2. On the Config Files Management page, select one or more configuration files.

   > **NOTE:** If any of the columns is not displayed by default, click the down arrow next to any of the displayed column headers and select the columns that you want displayed from the **Columns** list. The selected columns now appear on the Config Files Management page.

3. Select **Export Config Files** from the Actions menu.

   The Export Config File(s) dialog box opens, displaying the name of the file, the device name, and the configuration file versions stored. By default, the latest version is selected.

   > **NOTE:** If the Config File Name column is not displayed by default, click the down arrow next to any of the displayed columns and select the **Config File Name** column from the **Columns** list.

4. Select the appropriate version from the list that appears when you click next to the version number displayed in the **ConfigFile Version** column.

   The timestamp is displayed adjacent to the version number and indicates the date and time at which this version of the configuration was backed up.

5. Click **Export** on the Export Config File(s) dialog box.

   The Generating ZIP Archive dialog box appears, displaying a progress bar showing when the zip file is ready for downloading. The Opening deviceConfigFiles.zip dialog box opens, prompting you to view or save the file.

6. Save the zip file to your computer before closing either of the dialog boxes because the generated zip file is removed from the server immediately after the download is complete or when either of these two dialog boxes is closed. Refreshing or exiting the browser also removes the zip file from the server.

To view the contents of the device configuration file that you have just exported, extract the zip file and open the extracted file by using a text editor, such as Notepad. If you have exported the configuration file of more than one device, the extracted folder contains one configuration file for each device. The filename of the exported configuration file adheres to the following syntax: *device-name/IP address_version-number_timestamp in YYYYMMDD-hhmmss format-locale*.conf. For example, **Device1_3_20131104-082846-IST.conf**, where **Device1** is the device name, **3** is the version number of the configuration file that was exported, **20131104-082846** is the timestamp when the backup was taken in 24-hour format, and **IST** represents the time zone.

RELATED DOCUMENTATION

- Managing Configuration Files Overview | **938**
- Deleting Configuration Files | **962**
- Restoring Configuration Files | **958**
- Comparing Configuration Files | **953**
- Modifying Configuration Files | **955**
- Backing Up Configuration Files | **943**
- Viewing Audit Logs | **1117**

Deleting Configuration Files

You can delete device configuration files from Junos Space Network Management Platform if you no longer need them. You may want to delete the device configuration files in the following scenarios:

- When you want to use the device for a totally different purpose from what it is currently used for. In this case, because the configuration may have changed considerably, you cannot use the old backup configuration files to restore the device configuration.
- When the backup configuration file contains incorrect configuration information.

CAUTION: Before you proceed with the deletion, be aware that all versions of a backup configuration file are deleted from Junos Space Platform when you initiate a delete operation.

This delete operation does not delete the configuration file versions on the device.

To delete a configuration file:

1. On the Junos Space Platform UI, select **Configuration Files** > **Config Files Management**.

   The **Config Files Management** page appears, displaying all the configuration files saved in Junos Space Platform.

2. Select the configuration files that you want to delete and click the **Delete Configuration Files** icon.

   The **Delete Config File(s)** dialog box appears, listing the devices whose configuration files you have selected for deletion.

3. Click **Delete**.

   The **Delete Configuration Files** dialog box appears. This dialog box displays a message indicating that the delete action is successfully scheduled, and also displays a link to a job ID. You can click the job ID link to view details of the delete job on the Job Management page.

4. Click **OK** on the **Delete Configuration Files** dialog box to close the dialog box.

   The **Config Files Management** page reappears, displaying the remaining configuration files in Junos Space Platform.

When you delete a configuration file, an audit log entry is automatically generated. From the audit log entry, you can identify the user who initiated the delete operation, the IP address from which this task was initiated, and other details.

RELATED DOCUMENTATION

- Managing Configuration Files Overview | 938
- Restoring Configuration Files | 958
- Comparing Configuration Files | 953
- Modifying Configuration Files | 955
- Exporting Configuration Files | 960

PART 9

Jobs

Overview | **965**

Managing Jobs | **968**

CHAPTER 56

Overview

IN THIS CHAPTER

- Jobs Overview | 965

Jobs Overview

A job is an action that is performed on any object that is managed by Junos Space, such as a device, service, or user. The Jobs workspace lets you monitor the status of jobs that have run or are scheduled to run, in Junos Space Network Management Platform and all installed Junos Space applications. Jobs can be scheduled to run immediately or in the future.

By default, when you log in as a non-administrator, you can view only your own jobs, which include jobs triggered by you as well as jobs reassigned to you. However, at the time of creation or modification of a user account or remote profile, a User Administrator, can explicitly configure the user account or remote profile to view all jobs triggered by all users across all applications. For more information, see the topic "Creating Users in Junos Space Network Management Platform" on page 1035 or "Creating a Remote Profile" on page 1098, as needed.

Junos Space Platform also has a set of predefined user roles that can be assigned to a user to enable access to the various workspaces. For more information about the predefined roles in Junos Space Platform, see "Predefined Roles Overview" on page 999.

> **NOTE:** By default, a user with the Super Administrator or Job Administrator role can view all jobs triggered by all users across all applications.

Junos Space Platform maintains a history of job statuses for all jobs. When a job is initiated from a workspace, Junos Space Platform assigns a job ID that serves to identify the job (along with the job type) on the Job Management inventory page.

Table 119 lists some of the job types in Junos Space Platform.

NOTE: The job types listed in the table do not represent the entire list of job types you can manage in Junos Space Platform. Job types that appear in Junos Space Platform vary depending on what Junos Space applications are installed.

Table 119: Junos Space Platform Job Types

Junos Space Application	Supported Job Types
Network Management Platform	Add Node
	Discover Network Elements
	Update Device
	Delete Device
	Resync Network Element
	Role Assignment
	Audit Log Archive and Purge

From the Job Management page, you can select jobs and perform the following actions on them using the options on the Actions menu:

- **View Job Details**—View the job details. See "Viewing Jobs" on page 972.
- **Cancel Job**—Cancel scheduled or in-progress jobs. See "Canceling Jobs" on page 985.
- **Reassign Jobs**—Reassign scheduled or recurring jobs of a user to another user. See "Reassigning Jobs" on page 982.
- **Reschedule Job**—Reschedule a scheduled job. See "Rescheduling and Modifying the Recurrence Settings of Jobs" on page 978.
- **Retry on Failed Devices**—Retry a failed job on the devices. See "Retrying a Job on Failed Devices" on page 980.
- **Archive/Purge Jobs**—Archive and purge jobs from the Junos Space database. See "Archiving and Purging Jobs" on page 987.
- **View Recurrence**—Display details of recurring jobs, such as job start date and time, recurrence interval, end date and time, and job ID for each occurrence. See "Viewing Job Recurrence" on page 978.

- **Return to Application**—Return to the application page from which the job was initiated (if you have the correct permissions to do so). For example, if you selected a database backup recurrence job, then click **Return to Application** to go to the Database Backup and Restore page.
- **Delete Private Tags**—Delete private tags created by you. See "Deleting Tags" on page 1523.
- **Tag It**—Apply a tag to a job to segregate, filter, and categorize jobs. See "Tagging an Object" on page 1526.
- **View Tags**—Display tags applied to a job. See "Viewing Tags for a Managed Object" on page 1532.
- **UnTag It**—Remove tags from jobs. See "Untagging Objects" on page 1527.

> **NOTE:** From Junos Space Network Management Platform Release 15.1R1, device auto-resynchronization jobs are not displayed on the Job Management page. These jobs run in the background and you cannot cancel these jobs from the Junos Space UI. You can view the status of the auto-resynchronization job in the Managed Status column on the Device Management page or from the Device Count by Synchronization State widget on the Devices page. You can collect more information about these jobs from the **server.log** and **autoresync.log** files in the **/var/log/jboss/servers/server1** directory.
>
> You can view the auto-resynchronization jobs that were scheduled to execute before upgrading to Junos Space Platform Release 15.1R1, on the Job Management page. You can archive or purge these jobs by using the Archive and Purge Jobs workflow and selecting Resync Network Elements. For more information, see "Archiving and Purging Jobs" on page 987.

RELATED DOCUMENTATION

Viewing Jobs | **972**

Viewing Statistics for Jobs | **968**

Viewing Objects on Which a Job is Executed | **975**

Reassigning Jobs | **982**

Canceling Jobs | **985**

Viewing Job Recurrence | **978**

Archiving and Purging Jobs | **987**

CHAPTER 57

Managing Jobs

IN THIS CHAPTER

- Viewing Statistics for Jobs | **968**
- Viewing Your Jobs | **970**
- Viewing Jobs | **972**
- Viewing Objects on Which a Job is Executed | **975**
- Viewing Job Recurrence | **978**
- Rescheduling and Modifying the Recurrence Settings of Jobs | **978**
- Retrying a Job on Failed Devices | **980**
- Reassigning Jobs | **982**
- Canceling Jobs | **985**
- Clearing Your Jobs | **986**
- Archiving and Purging Jobs | **987**
- Common Error Messages in Device-Related Operations | **992**

Viewing Statistics for Jobs

The Jobs workspace statistics page displays graphs providing an overview of jobs triggered from all installed Junos Space applications. You can view the Jobs statistics page when you select Jobs from the task tree on the Junos Space Network Management Platform UI. The Jobs statistics page displays the following graphs:

- **Job Types** pie chart
- **State of Jobs Run** pie chart

- **Average Execution Time per Completed Job** bar chart

This topic includes the following tasks:

- Viewing the Types of Jobs That Are Run | **969**
- Viewing the State of Jobs That Have Run | **969**
- Viewing Average Execution Times for Jobs | **970**

Viewing the Types of Jobs That Are Run

The Job Types pie chart displays the percentages of all Junos Space Platform jobs that are of a particular job type. Each slice of the pie chart represents a job type and the percentage of time that the job type was run. The job type legend that is displayed on the right identifies each job type with a distinct color. Scroll down the list to see all job types. Mouse over a slice of the pie chart to view the job type title and the percentage of jobs that are of the selected job type.

To view details of jobs of a specific job type:

1. Click a job type slice on the **Job Types** pie chart.

   A filtered list of jobs of the selected job type is displayed on the Job Management page. For more information about the Job Management page, see "Viewing Jobs" on page 972.

2. Select **Jobs** from the breadcrumbs at the top of the Job Management page to return to the Jobs page.

Viewing the State of Jobs That Have Run

The State of Jobs Run pie chart displays the percentage of jobs that succeeded, are scheduled, are canceled, are in progress, or failed. Mouse over the pie chart to see the state and percentage of jobs run in each slice.

To view details of jobs in a particular state:

1. Click the job state slice on the **State of Jobs Run** pie chart.

   The filtered list of jobs in the selected state is displayed on the Job Management page. For more information about the Job Management page, see "Viewing Jobs" on page 972.

2. Select **Jobs** from the breadcrumbs at the top of the Job Management page to return to the Jobs page.

Viewing Average Execution Times for Jobs

Each bar on the Average Execution Time per Completed Job bar chart represents a job type and the average execution time for completed jobs of that job type in seconds. If there is space on the page, the job type appears at the bottom of each bar.

To view details of jobs of a specific job type:

1. Click the bar for the required job type, on the **Average Execution Time per Completed Job** bar chart.

   The filtered list of jobs in the selected state is displayed on the Job Management page. For more information about the Job Management page, see "Viewing Jobs" on page 972.

2. Select **Jobs** from the breadcrumbs at the top of the Job Management page to return to the Jobs page.

RELATED DOCUMENTATION

Viewing Jobs | **972**

Jobs Overview | **965**

Archiving and Purging Jobs | **987**

Viewing Your Jobs

You can view all your completed, in-progress, canceled, failed, and scheduled jobs in Junos Space Network Management Platform. Your jobs include jobs that were triggered by you as well as jobs that were reassigned to you. The My Jobs icon on the banner of the Junos Space Platform UI, allows you to quickly access summary and detailed information about all your jobs, from any workspace and from any task that you are currently performing.

To view your jobs:

1. In the banner of the Junos Space Platform UI, click the **My Jobs** icon located at the top right.

   The My Jobs dialog box appears, displaying your 25 most recent jobs.

   For each job, the following information is displayed:

   - Job ID
   - Job name
   - Job status
   - Date and time—The date and time displayed depends on the status of the job:
     - For jobs that are in progress, the date and time at which the job started are displayed.
     - For failed jobs, the date and time when the job failed are displayed.
     - For successful jobs, the date and time when the job succeeded are displayed.
     - For jobs that are scheduled for later, the date and time at which the job is scheduled to run are displayed.
   - Percentage of the job completed

2. (Optional) To view all your jobs, click **Manage My Jobs**.

   The Job Management page appears and displays a list of all your jobs.

3. (Optional) To view the details of a specific job, click the *job ID*.

   The Job Management page appears and displays the details of the selected job in a dialog box.

4. Click **Close** to exit the My Jobs page.

For troubleshooting, see the **/var/log/jboss/servers/server1/server.log** file.

RELATED DOCUMENTATION

Viewing Statistics for Jobs | **968**

Canceling Jobs | **985**

Jobs Overview | **965**

Clearing Your Jobs | **986**

Viewing Jobs

The Job Management inventory page displays all jobs that have been scheduled to run or have run from Junos Space Network Management Platform or other Junos Space applications. Scheduled and completed jobs appear in tabular format on the Job Management page. By default, jobs appear sorted by the Scheduled Start Time column. You can also sort by other columns on this page by clicking the appropriate column header. You can search for a particular job by entering the search criteria in the **Search** field.

For more information about how to manipulate inventory page data, see "Junos Space User Interface Overview" on page 89 in the *Junos Space User Interface Guide*.

To view jobs:

1. On the Junos Space Platform UI, select **Jobs > Job Management**.

   The Job Management page appears, displaying all jobs in tabular format. The fields displayed on the Job Management page are described in Table 120.

2. (Optional) Double-click a job entry to view the details for the selected job.

   The Job Details page appears. This page displays additional fields not displayed on the Job Management page.

   The Description column displays a View Details link if the job failed. Click the link to view why the job failed.

   The fields displayed on the Job Details page vary depending on the job. In the case of a Resync Network Elements job, the Job Details page displays the IP Address and Hostname fields, whereas for a Stage Script job, the Job Details page displays the Script Version and Script Name fields. Table 121 lists some of these fields.

   Currently, the jobs triggered for the following tasks exhibit this behavior:

   - Deleting scripts
   - Deleting a device
   - Resynchronizing network elements
   - Backing up configuration files
   - Deleting configuration files
   - Disabling scripts on devices
   - Enabling scripts on devices
   - Removing scripts from devices
   - Staging scripts on devices

Table 120: Fields on the Job Management Page

Field	Description
Job Type	The job type Job types indicate what tasks or operations are performed across Junos Space applications. Each Junos Space application supports certain job types.
ID	ID of the job
Domain	Domain from which the job is initiated
Name	Name of the job. For most jobs, the name is the job type with the job ID appended. However, for some jobs, the job name is supplied by the user as part of the workflow.
Percent	Percentage of the job that is completed
State	State of job execution: • **Scheduled**—The job is scheduled to run in the future. • **Success**—The job completed successfully. • **Failure**—The job failed and was terminated. • **In Progress**—The job is in progress. **NOTE:** When you add a Junos Space application or upgrade an existing Junos Space application, a progress bar is displayed. • **Cancelled**—The job was canceled by a user.
Parameters	Objects on which a job is performed or is scheduled to be performed
Scheduled Start Time	Start time that you specified for this job
Owner	Login name of the owner
Summary	Operations executed for the job
Recurrence	Scheduled recurrence
Retry Group ID	Job ID of the original job
Actual Start Time	Time when Junos Space Platform begins to execute the job. In most cases, the actual start time is the same as the scheduled start time.
End Time	Time when the job was completed or terminated if the job execution failed

Table 120: Fields on the Job Management Page *(continued)*

Previous Retry	Job ID of the previous job

Table 121: Fields on the Jobs Details Page

Field	Description
Status	Job status: Success, Failed, In Progress, or Cancelled.
Description	Details about why the job failed or whether it succeeded. This column displays information that is specific to the task that triggered this job.

Each job has a job status indicator. Table 122 defines these indicators.

Table 122: Job Icon Status Indicators

Job Status Indicator	Description
	The job was completed successfully.
	The job failed.
	The job was canceled by a user.
	The job is scheduled.
	The job is in progress.

RELATED DOCUMENTATION

- Viewing Statistics for Jobs | **968**
- Jobs Overview | **965**
- Canceling Jobs | **985**

Viewing Objects on Which a Job is Executed

A job is an action that is executed on any object that is managed by Junos Space, such as a device, service, or user.

From the Job Management inventory page, you can view the objects on which a job was performed or is scheduled to be performed. The **Parameters** column on this page provides you with this information. However, for jobs that are migrated from releases prior to Junos Space 13.3R1, this column does not display any information.

> **NOTE:** You can schedule certain types of jobs to run on devices that have been selected by using tags. The Parameters column on the Job Management page provides you with information about the target list of devices on which these jobs are scheduled to run. However, when the jobs are run, you may find that the devices on which they are run are different from the devices on which they were scheduled to run. This happens because the devices associated with a tag are resolved dynamically at runtime. If the devices associated with a tag have changed, then these jobs are executed on the devices that are associated with the tag at runtime. The type of jobs where you may see this behavior are:
>
> - Staging scripts on devices
> - Executing scripts on devices
> - Staging device images
> - Deploying device images
> - Staging script bundles on devices
> - Executing script bundles on devices
> - Running an operation
> - Backing up device configuration files

To view objects on which a job is executed:

1. On the Junos Space Platform UI, select **Jobs** > **Job Management**.

   The Job Management page displays the jobs in tabular view.

2. Select a job.

   The **Parameters** column for the selected job provides information about objects on which the job is performed.

   For example, when you select a Stage Scripts job, this column displays the device name and the script name associated with this job if you staged a single script on a single device. If you staged multiple

scripts on multiple devices, then this column displays the count of the scripts and the number of devices on which these scripts were staged.

3. Click the link in the **Parameters** column to view information about the objects.

   The Job Target dialog box appears, displaying the parameter types on separate tabs.

4. Click the tab that you are interested in to view the objects.

   If you staged multiple scripts on multiple devices, click the **Device(s)** tab to view the list of devices on which the scripts were staged. Click the **Script(s)** tab to view the scripts that were staged on these devices.

   NOTE:

   - It is not always necessary that the list of devices be displayed on the Device(s) tab. Script and image jobs may display the tag names or CSV filenames instead of devices. If you used a CSV file for staging or deploying an image, the filename of the CSV file is displayed instead of the devices on which the image is staged or deployed. This is true in the case of tag names as well.

     When you use tags to select the devices on which a job should be executed, you can select the Tag(s) tab to view the list of target devices on which the job is expected to be executed at the scheduled time.

   - For the following jobs, the Options tab displays options that you may have specified while triggering these jobs:
     - Deploying device images
     - Staging device images
     - Removing images from a staged device
     - Staging scripts on devices
     - Removing scripts from devices

5. Click **OK** in the Job Target dialog box to return to the Job Management page.

Table 123: Jobs that Support Viewing Objects on Which a Job is Executed

Workspace	Jobs
Device Management	Upload keys to devices.
	Modify authentication.
	Discover devices.
	Resynchronize devices.
CLI Configlets	Apply CLI Configlet.
Images and Scripts	Images • Stage an image on a device. • Verify the checksum. • Deploy a device image.
	Scripts: • Stage a script on devices. • Verify a script on devices. • Disable scripts on devices. • Enable scripts on devices. • Execute a script on devices. • Remove a script from devices.
	Operations: • Run operations.
	Script bundles: • Stage a script bundle on devices. • Execute a script bundle on devices. • Disable a script bundle on devices. • Enable a script bundle on devices.

RELATED DOCUMENTATION

Jobs Overview | 965

Viewing Job Recurrence

In Junos Space Network Management Platform, you can view the recurrence schedule of jobs that are configured to recur at regular intervals.

To view job recurrence information:

1. On the Junos Space Platform UI, select **Jobs > Job Management**.

   The Job Management page appears.

2. Select the job for which you want to view job recurrence information and select **View Recurrence** from the Actions menu.

   The View Job Recurrence dialog box appears, displaying the start date and time, recurrence interval, and end date and time of the selected job.

3. (Optional) Click the **Job ID** link to view all recurrences of the job.

4. Click **OK** on the View Job Recurrence dialog box to return to the Job Management page.

RELATED DOCUMENTATION

Backing Up the Junos Space Network Management Platform Database | 1308

Viewing Jobs | 972

Viewing Audit Logs | 1117

Rescheduling and Modifying the Recurrence Settings of Jobs

In Junos Space Network Management Platform, jobs are actions performed on managed objects. You can schedule jobs to run in the future, as well as create jobs that run periodically by setting recurrence intervals. From the Job Management page, you can reschedule a job and modify the recurrence settings to change the current schedule of the job.

You can reschedule jobs only in the following cases:

- Schedule and recurrence settings of a job can be modified if the job supports scheduling and recurrence, and it is currently in the Scheduled state.
- The schedule of a job in the Failed and Success states can be modified only if it is a recurring job.

- The recurrence setting of a scheduled job can be modified only if the job was created as a recurring job. This behavior is true for all scheduled jobs except the following:
  - Backing up configuration files
  - Backing up the MySQL and PostGreSQL database
  - Generating reports

To reschedule and modify the recurrence settings of jobs triggered by any user in Junos Space Platform, you must be assigned the privileges of a Job Administrator. As a Job User, you can reschedule or modify the recurrence settings of only those jobs that are scheduled by you.

To reschedule and modify the recurrence settings of a scheduled job:

1. On the Junos Space Platform UI, select **Jobs** > **Job Management**.

   The Job Management inventory page is displayed.

2. Select the job you want to reschedule and select **Reschedule Job** from the Actions menu.

   The Reschedule Job dialog box is displayed.

3. (Optional) Select the **Schedule at a later time** check box to reschedule the selected job.

   To specify the date and time when you want to run the job:

   a. Click the calendar icon and select the new date.

   b. Select the time from the drop-down list.

4. (Optional) Select the **Recurrence** check box to modify the job recurrence. By default, the job is executed once every week.

   To specify the new recurrence schedule:

   a. (Optional) Select the periodicity of recurrence from the **Repeats** list. The default is **Weekly**.

      If you select **Weekly** from the Repeats list, the **Repeat by** field appears, where you can select the check boxes for the days of the week that you want the job to recur.

   b. (Optional) Select the interval from the **Repeat every** list. The default is **1**.

   c. (Optional) Click the **On** option button in the **Ends** field to specify an end date for the job recurrence. If you select the **Never** option button, the job recurs endlessly until you cancel the job manually.

      To specify the date and time when you want to end the job recurrence:

      i. Click the calendar icon and select the date.

ii. Select the time from the drop-down list.

5. Click **Reschedule**.

   The job is rescheduled and you are redirected to the Job Management page.

RELATED DOCUMENTATION

Retrying a Job on Failed Devices | 980
Reassigning Jobs | 982

Retrying a Job on Failed Devices

Junos Space Network Management Platform allows you to retry jobs that did not complete successfully on devices on which they were configured to run. You can retry a failed job to ensure that the job succeeds on all target devices.

The following jobs can be retried if they fail:

- Applying configlets
- Backing up or restoring configuration files
- Validating or deploying a configuration
- Staging or executing a script
- Executing an operation
- Undeploying a template
- Deploying a template
- Deploying a device Image
- Staging a device image
- Verifying a device image
- Staging or executing a script bundle
- Backing up the database
- Resynchronizing the network elements

To retry a job that was not successful:

1. On the Junos Space Platform UI, select **Jobs** > **Job Management**.

   The Job Management page that appears displays the list of jobs.

2. Select the failed job that you want to retry.

3. From the Actions menu, select **Retry on Failed Devices**.

   The Retry Job dialog box appears.

   NOTE:
   - Only devices that belong to the domain to which you are logged in are displayed in this dialog box.
   - The fields displayed and the steps that you must follow to retry a job might vary depending on the job that you selected.

4. You can retry the job on all failed devices or only a few failed devices. Perform one of the following actions:

   - To retry the job on all devices listed on multiple pages, select **Select All Devices Across Pages**.

     If you select this option, the check boxes in the Select Applicable Devices table showing the device listings are unavailable.

   - If you want to run the job on a specific device, and you know the name of the device, enter the first few letters of the device name in the Search field and select the device from the suggestion list.

   - To run the job on one or more devices, select the device or devices from the **Select Applicable Devices** table.

     The following columns are displayed:

     - **Name**—Name of the device
     - **IP Address**—IP address of the device
     - **Job Status**—Status of the job: Failed/Failure, Success, or Canceled
     - **Description**—Description of the nature of the failure

5. (Optional) To view the devices on which the job cannot be retried, click the **View Inapplicable Devices** link.

   The View Inapplicable Devices page is displayed. This page shows all the devices on which the job cannot be retried.

6. (Optional) To retry the job later, select the **Schedule at a later time** check box.

   Select the date and time to run the job, from the date and time drop-down lists that appear.

7. Click **Run**.

   An information dialog box appears.

8. Click **OK**.

   The Job Management page is displayed. The retry job is listed on this page.

   If the Status column displays Success, the job you retried was executed successfully on the selected devices.

RELATED DOCUMENTATION

Jobs Overview | 965

Viewing Your Jobs | 175

Reassigning Jobs

You can reassign jobs owned by a user to another user within the same domain from the Job Management page by using the **Reassign Jobs** task. When you reassign jobs, you are transferring the ownership of these jobs from one user to another. For example, if you delete UserA, you might want to reassign the jobs of UserA to UserB to ensure that the scheduled and recurring jobs of UserA are monitored and taken to successful completion by UserB.

> **NOTE:** You can reassign only scheduled and recurring jobs. You cannot reassign jobs that are completed, in progress, or canceled.
>
> To reassign the jobs of one user to another user, you must be assigned the privileges of a Job Administrator.

To reassign a job:

1. On the Junos Space Platform UI, select **Jobs** > **Job Management**.

   The Job Management inventory page appears.

2. Select the jobs that you want to reassign.

3. Select **Reassign Jobs** from the Actions menu.

   The Reassign Jobs dialog box appears, listing the active users who are in the same domain as the user whose jobs you want to reassign. This dialog box does not list user accounts that are disabled.

4. Select the user to whom you want to reassign the jobs.

   Use the vertical scroll bar to navigate. You can also filter, or sort the users in ascending or descending order, to locate the user to whom you want to reassign the jobs.

5. Click **Reassign**.

   Depending on the role restrictions for the user you selected, one of the following can occur:

   - No jobs are reassigned.
   - Only some jobs are reassigned.
   - All jobs are reassigned.

6. Depending on the scenario you encounter, perform one of the following sets of tasks:

   - If none of the selected jobs can be reassigned to the user because of role restrictions, Junos Space Platform displays a warning dialog box indicating that the user does not have the necessary permissions. This dialog box lists the IDs and the types of the jobs that could not be reassigned. Click **Close** to exit the warning dialog box and return to the Job Management page.
   - If some of the selected jobs cannot be reassigned, a warning dialog box appears, indicating the number of jobs (out of the total selected jobs) that cannot be reassigned. This dialog box lists the IDs and the types of the jobs that cannot be reassigned. Perform one of the following actions:
     - To reassign the jobs that can be reassigned:

       a. Click **Confirm**.

          The jobs are reassigned and a dialog box appears informing you that the jobs have been successfully reassigned.

       b. Click **OK** to return to the Job Management page.

     - Click **Cancel** if you do not want to reassign any job.

       You return to the Job Management page.

   - If all the selected jobs can be reassigned, then a dialog box appears, informing you that all the jobs can be reassigned. Perform one of the following actions:
     - If you want to reassign the jobs:

       a. Click **Confirm**.

The jobs are reassigned and a dialog box appears informing you that the jobs have been successfully reassigned.

b. Click **OK** to return to the Job Management page.

- Click **Cancel** if you do not want to reassign any job.

  You return to the Job Management page.

If some or all jobs are reassigned, the **Owner** field on the Job Management page displays the new owner of the reassigned jobs.

When you reassign a job, an audit log entry is automatically generated and details about the reassigned job are recorded.

RELATED DOCUMENTATION

Jobs Overview | **965**

Canceling Jobs

Junos Space Network Management Platform allows you to cancel jobs that are scheduled for execution. You can also cancel jobs that are not completed for a long time or jobs that are hindering the execution of other jobs in the queue. You can cancel jobs from the Job Management page by using the **Cancel Job** task in the Actions menu.

Only jobs in the **Scheduled** or **In Progress** state can be canceled. If you select jobs in other states, the Cancel Job option is unavailable for selection.

If you are a user who is assigned the privileges of a Job Administrator, you can cancel jobs scheduled by any user. If you are a user who is assigned the privileges of a Job User, you can cancel only those jobs that are scheduled by you. If you are assigned a role that does not allow you to cancel any job, you cannot cancel any job in the Jobs workspace.

NOTE:

- If Junos Space Platform determines that the job operation cannot be interrupted, the job runs to completion; otherwise, the job is canceled.
- When you cancel jobs that are in-progress, some tasks associated with the job may be completed, depending on the stage at which you canceled the job. The status of the job on the Job Management page appears as **Cancelled**.
- Junos Space Platform does not clean up canceled jobs.

To cancel a job:

1. On the Junos Space Platform UI, select **Jobs** > **Job Management**.

   The Job Management page appears.

2. Click the job or multiple jobs to select the ones you want to cancel.

3. Select **Cancel Job** from the Actions menu.

   If any of the jobs you selected is in a state that you cannot cancel, the Cancel Job option is not available for selection.

   The **Cancel Job** dialog box appears listing the jobs you selected for cancellation.

4. Click **Yes** to confirm cancellation of selected jobs.

   When the Cancel Job task is completed, the Job Management page displays the state of the jobs as **Cancelled**.

   The **Summary** column provides information about the user who canceled the jobs.

RELATED DOCUMENTATION

Viewing Statistics for Jobs | 968

Jobs Overview | 965

Viewing Jobs | 972

Viewing Your Jobs | 175

Clearing Your Jobs

You can clear or remove jobs from the list of your jobs displayed in the My Jobs dialog box when the jobs are no longer of interest to you.

To remove the jobs that you initiated:

1. In the banner of the Junos Space Platform UI, click the **My Jobs** icon located at the top right.

   The My Jobs dialog box appears, displaying your 25 most recent jobs.

2. Perform one of the following actions:
   - Click the **Clear Job** icon that appears to the right of the job to remove that job from the list of jobs displayed.
   - Click the **Clear All My Jobs** icon at the top of the My Jobs dialog box to clear all the jobs displayed.

   NOTE: Clearing a job from the My Jobs dialog box does not affect the job itself, it only removes the job from the list of jobs displayed in the My Jobs dialog box.

3. Click **Close** to exit the My Jobs dialog box.

RELATED DOCUMENTATION

Viewing Your Jobs | 175

Jobs Overview | 965

Archiving and Purging Jobs

Over a period of time, the number of job records in the Junos Space Platform database increases. Accumulation of job records in the database could adversely affect the server performance. Because many of the jobs have no relevance after a few hours of their creation or execution, you can purge records of such jobs to avoid strain on the system. If you want to retain the job records for future reference, you can archive the records before purging the records from the system. When you archive the records, the records are saved as a CSV file. You can choose to retain the archived records locally or on a remote server.

You can purge or archive and purge the jobs (successful or not) completed until a time you specify or until the time you initiate the purging or archiving and purging. You must have Super Administrator or Job Administrator role assigned to your account to perform this task.

When you archive jobs locally, the archive files are stored in the default **/var/lib/mysql/archive** directory on the active Junos Space node. When you archive jobs to a remote server, the archive files are stored in the directory that you specify.

The default filename for an archive is **JunosSpaceJobArchive_*date_time*.zip**, where *date* specifies the year, month, and day, in the *yyyy-mm-dd* format; and *time* specifies hours, minutes, and seconds, in the *hh-mm-ss* format.

This topic includes the following tasks:

- Purging Jobs Without Archiving | **987**
- Archiving Jobs to a Local Server and Purging the Jobs from the Database | **989**
- Archiving Jobs to a Remote Server and Purging the Jobs from the Database | **990**

Purging Jobs Without Archiving

From Release 17.2R1 onward, Junos Space Platform enables you to purge jobs without archiving the jobs.

To purge Junos Space Platform jobs without archiving the jobs:

1. On the Junos Space Platform UI, select **Jobs** > **Job Management**.

   The Job Management page appears.

2. Click the **Archive/Purge Jobs** icon.

   The Archive/Purge Jobs dialog box appears.

3. Select the job type from the **Job Type** list. You can select any job type from the list to purge jobs of that job type, or select the **All** option to purge all jobs from the database.

Job types of jobs that are already initiated or completed in Junos Space appear on the **Job Type** list. In-progress and scheduled jobs are not archived.

4. For the **Purge Jobs Before** field, select a date and time to specify the time up to which all jobs are to be purged from the Junos Space Platform database. You can specify only a date and time in the past.

   > **NOTE:** If you do not specify a date and time in the **Purge Jobs Before** field, Junos Space Platform purges or archives and purges all jobs up to the time that you initiate the purge or archive and purge operation.

5. To purge jobs from all accessible domains, select the **Purge Jobs from all accessible domains** check box.

6. Clear the **Archive Jobs Before Purging** check box. This check box is selected by default.

7. To schedule the purge operation, select the **Schedule at a later time** check box and specify a later start date and time for the archive-and-purge operation.

   > **NOTE:** The date and time that you specify in the Archive/Purge Jobs dialog box is the date and time on the client computer. Junos Space Platform maps the specified date and time to the Junos Space server time and schedules the archive-and-purge task.

   If you do not select **Schedule at a later time**, the specified job is initiated immediately when you click **Submit**.

8. Click **Submit**.

   The Jobs Archive and Purge Job Information page appears.

   > **NOTE:** If sufficient space is not available in the default directory, Junos Space displays an error message and the archive-and-purge task fails.

9. Perform one of the following actions:

   - To view job details for the archive-and-purge operation, click the **Job ID** link in the Jobs Archive and Purge Job Information dialog box.
   - Click **OK** to close the Jobs Archive and Purge Job Information dialog box.

Archiving Jobs to a Local Server and Purging the Jobs from the Database

Before you purge jobs, you can archive the jobs to the local server. The local server is the server that functions as the active node in the Junos Space fabric.

To archive Junos Space Platform jobs to the local server and then purge the jobs from the database:

1. On the Junos Space Platform UI, select **Jobs** > **Job Management**.

   The Job Management page appears.

2. Click the **Archive/Purge Jobs** icon.

   The Archive/Purge Jobs dialog box appears.

3. Select the job type from the **Job Type** list. You can select any job type from the list to archive jobs of that job type, or select the **All** option to archive all jobs and then purge them from the database.

   Job types of jobs that are already initiated or completed in Junos Space appear on the **Job Type** list. In-progress and scheduled jobs are not archived.

4. For the **Purge Jobs Before** field, select a date and time to specify the date up to which all jobs are to be archived and purged from the Junos Space Platform database. You can specify only a date and time in the past.

   > **NOTE:** If you do not specify a date and time in the Archive Jobs Before field, Junos Space Platform archives and purges all jobs up to the time that you initiate the archive and purge operation.

5. To purge jobs from all accessible domains, select the **Purge Jobs from all accessible domains** check box.

   If you do not select this check box, Junos Space Platform purges jobs only from the current domain of the user.

6. To archive and purge the jobs, select the **Archive Jobs Before Purging** check box and complete the following steps:

   a. For the **Archive Mode** field, select **Local** from the list.

7. To schedule the archive-and-purge operation, select the **Schedule at a later time** check box and specify a later start date and time for the archive-and-purge operation.

> **NOTE:** The date and time that you specify in the Archive/Purge Jobs dialog box is the date and time on the client computer. Junos Space Platform maps the specified date and time to the Junos Space server time and schedules the archive-and-purge task.

If you do not select **Schedule at a later time**, the specified job is initiated immediately when you click **Submit**.

8. Click **Submit**.

   The Jobs Archive and Purge Job Information page appears.

   > **NOTE:** If sufficient space is not available in the default directory, Junos Space displays an error message and the archive-and-purge task fails.

9. Perform one of the following actions:
   - To view job details for the archive-and-purge operation, click the **Job ID** link in the Jobs Archive and Purge Job Information dialog box.
   - Click **OK** to close the Jobs Archive and Purge Job Information dialog box.

Archiving Jobs to a Remote Server and Purging the Jobs from the Database

You can also choose to archive jobs to a remote server before purging the jobs from the Junos Space Platform database. Junos Space Platform uses Secure Copy Protocol (SCP) to copy the files in this case.

To archive jobs to a remote server and then purge them from the Junos Space Platform database:

1. On the Junos Space Platform UI, select **Jobs** > **Job Management**.

   The Job Management page appears.

2. Click the **Archive/Purge Jobs** icon. The Archive/Purge Jobs dialog box appears.

3. Select the job type from the **Job Type** list. You can select any job type from the list to archive jobs of that job type, or select the **All** option to archive all jobs and then purge them from the database.

   Job types of jobs that are already initiated or completed in Junos Space appear on the **Job Type** list. In-progress and scheduled jobs are not archived.

4. For the **Purge Jobs Before** field, select a date and time to specify the date up to which all jobs are to be archived and purged from the Junos Space Platform database. You can specify only a date and time in the past.

   NOTE: If you do not specify a date and time in the Archive Jobs Before field, Junos Space Platform archives and then purges from the database all jobs up to the time that you initiated the operation.

5. To purge jobs from all accessible domains, select the **Purge Jobs from all accessible domains** check box.

   If you do not select this check box, Junos Space Platform purges jobs only from the current domain of the user.

6. To archive and purge the jobs, select the **Archive Jobs Before Purging** check box and complete the following steps:

   a. For the **Archive Mode** field, select **Local** from the list.

   b. In the **User** field, enter a valid username to access the remote host server.

   c. In the **Password** field, enter a valid password to access the remote host server.

   d. In the **Confirm Password** field, reenter the password you entered in the previous step.

   e. In the **Machine IP** field, enter the IP address of the remote host server.

   f. In the **Directory** field, enter a directory path on the remote host server for the archived files.

      NOTE: The directory path must already exist on the remote host server. If sufficient space is not available in the specified directory, Junos Space displays an error message and the archive-and-purge task fails.

7. To schedule the archive-and-purge operation, select the **Schedule at a later time** check box and specify a later start date and time for the archive-and-purge operation.

> **NOTE:** The date and time that you specify in the Archive/Purge Jobs dialog box is the date and time on the client computer. Junos Space Platform maps the specified date and time to the Junos Space server time and schedules the archive-and-purge task.

If you do not select **Schedule at a later time**, the specified job is initiated immediately when you click **Submit**.

8. Click **Submit**.

   The Jobs Archive and Purge dialog box displays the file location and the name of the remote server.

9. Click **Continue** in the Jobs Archive and Purge dialog box to archive and purge the jobs.

   Junos Space Platform displays the Jobs Archive and Purge Job Information dialog box.

10. Perform one of the following actions:

    - To view job details for the archive-and-purge operation, click the **Job ID** link in the Jobs Archive and Purge Job Information dialog box.
    - Click **OK** to close the Jobs Archive and Purge Job Information dialog box.

RELATED DOCUMENTATION

Jobs Overview | **965**

Viewing Your Jobs | **175**

Viewing Jobs | **972**

Viewing Job Recurrence | **978**

Common Error Messages in Device-Related Operations

From Release 17.2R1 onward, Junos Space Network Management Platform provides descriptive error messages that explain the reasons for common errors in device-related operations. The error message is recorded in the job details of the corresponding job on Job Management page.

The error messages and suggested resolutions are listed in Table 124.

Table 124: Comon Error Messages in Device-Related Operations

Error Message	Suggested Solution
Unable to establish connection with the device (Device Id: *device_id*). Device is down, not reachable, or unable to accept requests.	If the device is in UP state, retry the operation. If the device is in DOWN state, wait for the device to be in UP state and retry the operation.
Unable to establish connection with the device (Device Id: *device_id*) because all channels are busy.	Retry the operation.
Unable to establish connection with the device (Device Id: *device_id*). <execution message thrown from J2SSH library>	Retry the operation. If the issue persists, download troubleshooting logs and please contact the Juniper Technical Assistance Center.
Unable to close the channel with the device (Device Id: *device_id*). Channel might be closed already.	This error can be ignored if it occurs intermittently. If the issue persists, download troubleshooting logs and please contact the Juniper Technical Assistance Center.
Unable to apply configuration changes on the device because the device configuration is being modified by another user and is locked. Commit or rollback the pending configuration changes.	Roll back uncommitted changes from the device.
Unable to get configuration or apply configuration changes on the device because the device returns an unknown error. Error Message from device: <RPC error message from device>	Retry the operation. If the issue persists, download troubleshooting logs and please contact the Juniper Technical Assistance Center.
Unable to apply configuration changes to the device as the configuration being pushed has invalid value. This could be due to an invalid reference to a non-existent key. If the configuration is generated by Junos Space, make sure that the configuration in Junos Space is in sync with that of the device.	If the configuration is generated by Junos Space, resynchronize the device and retry the operation. If the configuration is manually generated, review the configuration for invalid parameters and retry the operation with the corrected configuration.

RELATED DOCUMENTATION

Viewing Jobs | 972

PART 10

Role-Based Access Control

Overview | **995**

Roles | **997**

User Accounts | **1033**

User Groups | **1069**

Domains | **1077**

Remote Profiles | **1098**

API Access Profiles | **1102**

User Sessions | **1106**

CHAPTER 58

Overview

IN THIS CHAPTER

- Role-Based Access Control Overview | 995

Role-Based Access Control Overview

Junos Space Network Management Platform grants access and management privileges only to those users validated by its authentication process and given permissions by its authorization process.

A Junos Space Super Administrator or User Administrator creates users and then assigns them one or more roles so that they are able to access and manage tasks and objects within workspaces in Junos Space Platform. The roles determine which workspace or workspaces a user can access and which tasks the user can perform within the workspace or workspaces.

As a Junos Space Super Administrator or User Administrator, you can also create and assign API Access Profiles to restrict users from executing remote procedure call (RPC) commands that are potentially unsafe for or harmful to your network. Rules are added to an API Access Profile as XPath expressions that determine whether or not an RPC command is safe to be executed.

User Authentication

Through authentication, Junos Space Network Management Platform validates users on the basis of passwords or certificates. Junos Space Network Management Platform supports both local and remote user authentication. When a user tries to access Junos Space Network Management Platform, the user can be authenticated locally by confirming that the password entered by the user at login matches the password stored in the Junos Space Platform database or remotely through a RADIUS or TACACS+ server. For information about configuring RADIUS and TACACS+ servers for remote authentication and authorization, see “Configuring a RADIUS Server for Authentication and Authorization” on page 1473 and “Configuring a TACACS+ Server for Authentication and Authorization” on page 1475.

Junos Space Network Management Platform also supports certificate-based user authentication and X.509 certificate parameter–based user authentication. Instead of authenticating a user on the basis of the user’s credentials, you can authenticate a user on the basis of the user’s certificate, which is considered more

secure. For more information about certificate-based authentication or certificate parameter–based authentication, see “Certificate Management Overview” on page 1426.

RBAC Enforcement

With role-based access control (RBAC) enforcement, a Junos Space Super Administrator or User Administrator defines the workspaces that users can access, the system resources that users can view and manage, and the tasks available to users within a workspace. RBAC is enforced in the Junos Space user interface navigation hierarchy by workspace, task group, and task. A user can access only those portions of the navigation hierarchy that are explicitly granted through access privileges. The following sections describe RBAC enforcement behavior at each level of the user interface navigation hierarchy.

RBAC Enforcement by Workspace

The Junos Space user interface provides a task-oriented environment in which a collection of related tasks is organized by workspace. For example, the Users workspace defines the group of tasks related to managing users and roles. These tasks include creating, modifying, and deleting users, and assigning roles. Enforcement by workspace ensures that a user can view only those workspaces that contain the tasks that the user has permissions to execute. For example, a user who is assigned the device manager role, which grants access privileges to all tasks in the Devices workspace, can access only the Devices workspace. No other workspaces are visible to this user unless other roles are assigned to this user. If a user is assigned a role that grants access privileges to some tasks in a workspace, the user can view all the tasks in the workspace, but execute only the tasks for which permissions have been granted.

RBAC Enforcement Not Supported on the Getting Started Page

RBAC enforcement is not enabled for the contents of the Getting Started page. Consequently, a user who does not have certain access privileges can still view the steps displayed on the Getting Started page. For example, a user without privileges to manage devices still sees the Discover Devices step. However, when the user clicks the step, Junos Space Network Management Platform displays an error message to indicate that the user does not have the permission to access the workspace or tasks to which the step is linked.

RELATED DOCUMENTATION

- Configuring Users to Manage Objects in Junos Space Overview | **1033**
- Predefined Roles Overview | **999**
- Creating Users in Junos Space Network Management Platform | **1035**
- Creating a Remote Profile | **1098**
- Creating an API Access Profile | **1102**
- Viewing User Statistics | **1068**
- Viewing Users | **1054**
- Configuring a RADIUS Server for Authentication and Authorization | **1473**

CHAPTER 59

Roles

IN THIS CHAPTER

- Roles Overview | **998**
- Predefined Roles Overview | **999**
- Creating a User-Defined Role | **1022**
- Managing Roles | **1024**
- Modifying User-Defined Roles | **1026**
- Deleting User-Defined Roles | **1027**
- Cloning Predefined and User-Defined Roles | **1028**
- Exporting User-Defined Roles from Junos Space Network Management Platform | **1030**
- Importing Roles to Junos Space Network Management Platform | **1031**

Roles Overview

A role is a specific set of tasks that can be assigned to users in Junos Space Network Management Platform. Each user is assigned one or more roles by the Super Administrator or User Administrator depending on the tasks the user is expected to perform. A user represents an individual in a security domain who is authorized to log in to Junos Space Platform and perform application workspace tasks according to assigned roles. The roles can be either predefined or user-defined.

The administrator can create a user account and assign tasks based on read-only predefined roles and read/write user-defined roles. See "Creating Users in Junos Space Network Management Platform" on page 1035 and "Predefined Roles Overview" on page 999. You can create user-defined roles and then create a user account, or create a user account and then modify the account. You can also use an existing user account as a template to assign roles to users with similar job types.

The **Role Based Access Control** > **User Accounts** task allows the Super Administrator or User Administrator to manage all roles by performing the following tasks:

- View all predefined and user-defined roles on the **Role Based Access Control** > **Roles** inventory page. See "Managing Roles" on page 1024.
- Create user-defined roles from the **Role Based Access Control** > **Roles** > **Create Role** task. See "Creating a User-Defined Role" on page 1022.
- Modify user-defined roles by using **Modify Role** on the **Role Based Access Control** > **Roles** inventory page. See "Modifying User-Defined Roles" on page 1026.
- Delete user-defined roles by using **Delete Roles** on the **Role Based Access Control** > **Roles** inventory page. See "Deleting User-Defined Roles" on page 1027.
- Tag predefined and user-defined roles to group them for performing actions simultaneously. Select **Tag It** from the Actions menu on the **Role Based Access Control** > **Roles** inventory page. See "Tagging an Object" on page 1526.
- View all tags that exist on roles by selecting **View Tags** from the Actions menu on the **Role Based Access Control** > **Roles** inventory page. See "Viewing Tags for a Managed Object" on page 1532.
- Import roles in an XML file to Junos Space Network Management Platform. See "Importing Roles to Junos Space Network Management Platform" on page 1031

RELATED DOCUMENTATION

Role-Based Access Control Overview | **995**

Predefined Roles Overview | **999**

Creating Users in Junos Space Network Management Platform | **1035**

Managing Roles | **1024**

Creating a User-Defined Role | 1022
Modifying User-Defined Roles | 1026
Deleting User-Defined Roles | 1027
Cloning Predefined and User-Defined Roles | 1028

Predefined Roles Overview

Junos Space Network Management Platform provides predefined roles that you can assign to users to define administrative responsibilities and specify the management tasks that a user can perform within applications and workspaces.

To assign roles to other users in Junos Space Network Management Platform, a user must be a Super Administrator or User Administrator.

Each predefined role defines a set of tasks for a single workspace, except the Super Administrator role, which defines all tasks for all workspaces. By default, Junos Space Network Management Platform provides read privileges on all objects associated with the task groups defined in a predefined role.

Table 125 and Table 126 show the Junos Space Network Management Platform predefined roles (A through Q and R through Z respectively) and corresponding tasks available for installed Junos Space applications.

> **NOTE:** The predefined roles that appear in the Junos Space Network Management Platform release that you are using depend on the Junos Space applications that you have installed. For the latest predefined roles, see **Network Management Platform** > **Role Based Access Control** > **Roles**.
>
> For information about predefined roles for a specific Junos Space application, refer to the documentation for that Junos Space application.

Table 125: Predefined Roles (A through Q) for the Junos Space Network Management Platform

Predefined Role	Task Group and Tasks	Application > Workspace
Audit Log Administrator	Audit Log • Archive/Purge Logs • Export Audit Logs	Network Management Platform > Audit Logs

Table 125: Predefined Roles (A through Q) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace

CLI Configlets Manager	CLI Configlets
	• Configlets
	  ◦ Create CLI Configlet
	  ◦ Delete CLI Configlets
	  ◦ Compare CLI Configlet Versions
	  ◦ View CLI Configlet Details
	  ◦ Modify CLI Configlet
	  ◦ Clone CLI Configlet
	  ◦ Apply CLI Configlet
	  ◦ Export Selected CLI Configlets
	  ◦ Export All CLI Configlets
	  ◦ Import CLI Configlet
	  ◦ Assign CLI Template to Domain
		Network Management Platform > CLI Configlets

CLI Configlets Manager	Devices
	• Device Management
	  ◦ Secure Console
	  ◦ Apply CLI Configlet
		Network Management Platform > Devices

CLI Configlets Operator	CLI Configlets • Configlets ◦ Apply CLI Configlet	Network Management Platform > CLI Configlets
CLI Configlets Operator	Devices • Device Management • Secure Console • Apply CLI Configlet	Network Management Platform > Devices

Table 125: Predefined Roles (A through Q) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace

Configuration File Manager	Configuration Files
	• Config Files Management
	  ◦ Backup Configuration Files
	  ◦ Delete Configuration Files
	  ◦ Restore Configuration Files
	  ◦ Compare Configuration File Versions
	  ◦ Export Configuration File
	  ◦ Modify Configuration File
		Network Management Platform > Configuration Files

Configuration Filter Manager	CLI Configlets
	• Configuration Filter
	  ◦ Create Configuration Filter
	  ◦ Modify Configuration Filter
	  ◦ Delete Configuration Filter
	  ◦ Assign Configuration Filter to Domain
		Network Management Platform > CLI Configlets

Configuration Filter Manager	Devices • Device Management ◦ Device Configuration • Secure Console • Create/Edit/Delete Filter	Network Management Platform > Devices

Configuration View Manager	CLI Configlets
	• Configuration View
	  ◦ Create Configuration View
	  ◦ Modify Configuration View
	  ◦ Delete Configuration View
	  ◦ View Configuration View Details
	  ◦ Export Configuration Views
	  ◦ Import Configuration Views
		Network Management Platform > CLI Configlets

Table 125: Predefined Roles (A through Q) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace

Configuration View Manager	Devices
	• Device Management
	  ◦ Device Configuration
	  ▪ View Active Configuration
	• Secure Console
		Network Management Platform > Devices

Configuration View Operator	• CLI Configlets ◦ Configuration View	Network Management Platform > CLI Configlets

Configuration View Operator	• Devices
	  ◦ Device Management
	  ▪ Device Configuration
	  ▪ View Active Configuration
	  ◦ Secure Console
		Network Management Platform > Devices

Device Image Manager	Devices
	• Device Adapter
	  ◦ Add Adapter
	  ◦ Upgrade Adapter
	  ◦ Delete Adapter
		Network Management Platform > Devices

Device Image Manager	Images and Scripts
	• Images
	  ◦ Import Images
	  ◦ View Deployed Results
	  ◦ Modify Device Image
	  ◦ Delete Device Images
	  ◦ Stage Image on Device
	  ◦ MD5 Validation Result
	  ◦ Verify Image on Devices
	  ◦ Deploy Device Image
	  ◦ Undeploy JAM Package from Device
	  ◦ Remove Image from Staged Device
	  ◦ View Associated Devices
	  ◦ Assign Image to Domain
		Network Management Platform > Images and Scripts

Table 125: Predefined Roles (A through Q) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace

Device Images Read Only User	Images and Scripts
	• Images
	  • View Deployed Results
	  • View Associated Devices
		Network Management Platform > Images and Scripts

Device Manager	CLI Configlets • View CLI Configlet Details • Apply CLI Configlet	Network Management Platform > CLI Configlets

Table 125: Predefined Roles (A through Q) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace
Device Manager		Network Management Platform > Devices

Table 125: Predefined Roles (A through Q) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace

	Devices
	• Device Management
	  • Device Configuration
	  • View Active Configuration
	  • Create/Edit/Delete Filter
	  • Resolve Out-of-band Changes
	  • View/Assign Shared Objects
	  • View Configuration Change Log
	  • View Template Deployment
	  • Modify Unmanaged Device Configuration
	  • Review/Deploy Configuration
	  • Validate on Device
	  • Approve
	  • Reject
	  • Deploy
	  • Modify Configuration
	  • Assign Device to Domain
	  • Device Inventory
	  • Export Physical Inventory
	  • View Associated Scripts
	  • View License Inventory
	  • View Logical Interfaces
	  • View Physical Interfaces
	  • View Physical Inventory
	  • View Script Executions
	  • View/Acknowledge Inventory Changes
	  • View Software Inventory
	  • View Staged Images
	  • Delete Staged Images
	  • Verify Checksum
	  • Device Operations
	  • Create LSYS
	  • Manage Device Partition
	  • Create Partition
	  • Modify Partition	

Table 125: Predefined Roles (A through Q) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace
	• Delete Partition • Assign Partition to Domain • Delete Devices • Looking Glass • Export Looking Glass Results • Put in RMA State • Reactivate from RMA • Resynchronize with Network • Execute Scripts • Reboot Devices • Apply CLI Configlet • Clone Device • Activate Modeled Device • View/Download Configlet • Modify Serial Number • Device Access • Launch Device WebUI • Modify Authentication • Modify Device Target IP • Acknowledge Device Fingerprint • SSH to Device • Resolve Key Conflict • Manage Customized Attributes • Add Label • Delete Label • Upload Keys to Devices • Modify Serial Number • Secure Console • Modify Device Configuration • Device Discovery • Discover Targets • Specify Probes • Specify Credentials • Specify Fingerprints	

Table 125: Predefined Roles (A through Q) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace

	• Model Devices
	  ◦ Create Modeled Instance
	  ◦ Add More Devices
	  ◦ View Modeled Instance
	  ◦ View Modeled Device Status
	  ◦ View Configlet
	  ◦ Download Configlet
	  ◦ Delete Modeled Instances
	  ◦ Connection Profiles
	  ▪ Create Connection Profile
	  ▪ Modify Connection Profile
	  ▪ View Connection Profile
	  ▪ Delete Connection Profiles
	  ▪ Clone Connection Profile
	• Unmanaged Devices
	• View Alarms
	• View Performance Graphs
	• Device Discovery Profiles
	  ◦ Create Device Discovery Profile
	  ◦ Modify Device Discovery Profile
	  ◦ Clone Device Discovery Profile
	  ◦ Delete Device Discovery Profiles
	  ◦ Run Now Device Discovery Profile	

Table 125: Predefined Roles (A through Q) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace

Device Script Manager	Images and Scripts
	• Scripts
	  ◦ Compare Script Versions
	  ◦ Import Script
	  ◦ View Execution Results
	  ◦ Modify Script
	  ◦ Modify And Stage Scripts on Device
	  ◦ Delete Scripts
	  ◦ Stage Scripts on Devices
	  ◦ View Associated Devices
	  ◦ Verify Scripts on Devices
	  ◦ Verification Results
	  ◦ Enable Scripts on Devices
	  ◦ Disable Scripts on Devices
	  ◦ Remove Scripts from Devices
	  ◦ Execute Script on Devices
	  ◦ Export Scripts
	  ◦ Modify Scripts Type
	  ◦ Assign Script to Domain
	• Script Bundles
	  ◦ Create Script Bundle
	  ◦ Embedded Script
	  ◦ Modify Script Bundle
	  ◦ Delete Script Bundles
	  ◦ Stage Script Bundle on Devices
	  ◦ View Associated Devices
	  ◦ Enable Script Bundle on Devices
	  ◦ Disable Script Bundle on Devices
	  ◦ Execute Script Bundle on Devices
		Network Management Platform > Images and Scripts

Device Script Operator	Devices • Device Management • Secure Console	Network Management Platform > Devices

Table 125: Predefined Roles (A through Q) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace

Device Script Operator	Images and Scripts
	• Scripts
	  ◦ Compare Script Versions
	  ◦ Execute Script on Devices
		Network Management Platform > Images and Scripts

Device Script Read Only User	Images and Scripts
	• Scripts
	  ◦ Compare Script Versions
	  ◦ View Execution Results
	  ◦ View Associated Devices
	  ◦ Export Scripts
	• Script Bundles
		Network Management Platform > Images and Scripts

Domain Administrator	Devices • Device Management • Secure Console	Network Management Platform > Devices

Domain Administrator	Role Based Access Control
	• Domains
	  ◦ Create Domain
	  ◦ Modify Domain
	  ◦ Delete Domain
	  ◦ Export Domain
	  ◦ Assign Devices to Domain
	  ◦ Assign Domain to Users
	• User Accounts
		Network Management Platform > Role Based Access Control

Table 125: Predefined Roles (A through Q) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace
FMPM Manager	Network Monitoring • Node List ◦ Resync Nodes • Search • Outages • Dashboard • Events • Alarms • Notifications • Assets • Reports • Charts • Topology • Admin	Network Management Platform > Network Monitoring
FMPM Read Only User	Network Monitoring • Node List ◦ Resync Nodes • Search • Outages • Dashboard • Events • Alarms • Notifications • Assets • Reports • Charts • Topology	Network Management Platform > Network Monitoring

Table 125: Predefined Roles (A through Q) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace

Job Administrator	Jobs
	• Job Management
	  ◦ Cancel My Job
	  ▪ Cancel Any Job
	  ◦ Reassign Jobs
	  ◦ Archive/Purge Jobs
	  ◦ Reschedule Job
	  ◦ View Recurrence
		Network Management Platform > Jobs

Job User	Jobs
	• Job Management
	  ◦ Cancel My Job
	  ◦ Reschedule Job
	  ◦ View Recurrence
		Network Management Platform > Jobs

Operation Manager	Devices
	• Device Adapter
	  ◦ Add Adapter
	  ◦ Upgrade Adapter
	  ◦ Delete Adapter
		Network Management Platform > Devices

Table 125: Predefined Roles (A through Q) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace
Operation Manager		Network Management Platform > Images and Scripts

Table 125: Predefined Roles (A through Q) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace

	Images and Scripts
	• Images
	  ◦ Import Images
	  ◦ View Deployed Results
	  ◦ Modify Device Image
	  ◦ Delete Device Images
	  ◦ Stage Image on Device
	  ◦ MD5 Validation Result
	  ◦ Verify Image on Devices
	  ◦ Deploy Device Image
	  ◦ Remove Image from Staged Device
	  ◦ View Associated Devices
	  ◦ Assign Image to Domain
	• Scripts
	  ◦ Compare Script Versions
	  ◦ Import Script
	  ◦ View Execution Results
	  ◦ Modify Script
	  ◦ Modify And Stage Scripts on Device
	  ◦ Delete Scripts
	  ◦ Stage Scripts on Devices
	  ◦ View Associated Devices
	  ◦ Verify Scripts on Devices
	  ◦ Verification Results
	  ◦ Enable Scripts on Devices
	  ◦ Disable Scripts on Devices
	  ◦ Remove Scripts from Devices
	  ◦ Execute Script on Devices
	  ◦ Export Scripts
	  ◦ Modify Scripts Type
	  ◦ Assign Script to Domain
	• Script Bundles
	  ◦ Create Script Bundle
	  ◦ Embedded Script	

Table 125: Predefined Roles (A through Q) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace

	• Modify Script Bundle
	• View Associated Devices
	• Enable Script Bundle on Devices
	• Disable Script Bundle on Devices
	• Delete Script Bundles
	• Stage Script Bundle on Devices
	• Execute Script Bundle on Devices
	• Assign Script Bundle to Domain
	• Operations
	  • Create Operation
	  • Clone Operation
	  • Modify Operation
	  • Delete Operations
	  • Import Operations
	  • Export Operations
	  • Run Operation
	  • View Operation Results
	  • Assign Operation to Domain	

Table 126: Predefined Roles (R through Z) for the Junos Space Network Management Platform

Predefined Role	Task Group and Tasks	Application > Workspace

Report Administrator	Reports
	• Generated Reports
	  • Delete Generated Report
	  • View Generated Report
		Network Management Platform > Reports

Table 126: Predefined Roles (R through Z) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace

Report Definition Administrator	Reports
	• Report Definitions
	  ◦ Create Report Definition
	  ◦ Modify Report Definition
	  ◦ Delete Report Definition
	  ◦ Clone Report Definition
	  ◦ View Report Definition
	  ◦ Generate Report
	  ◦ Assign Report Definition to Domain
		Network Management Platform > Reports

Super Administrator	Manages all Junos Space Network Management Platform task groups and tasks. See **Network Management Platform** > **Users** > **Roles** > **Super Administrator** > **View Detail** for a list of tasks that are currently supported.	All Junos Space Network Management Platform workspaces

Table 126: Predefined Roles (R through Z) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace
System Administrator		Network Management Platform > Administration

Table 126: Predefined Roles (R through Z) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace

	Administration
	• Fabric
	  • Extended Periods of High CPU
	  • List of HPROF Files
	  • Large Database Tables
	  • Last JBoss Restarted Time
	  • Device Management Sessions
	  • Add Fabric Node
	  • Delete Fabric Node
	  • View Fabric Node Alarms
	  • Device Load Balancing
	  • Shutdown/Reboot Node(s)
	  • Space Node Settings
	  • SNMP Configuration
	  • SNMP Manager
	  • NAT Configuration
	  • Check For File Integrity
	  • Reset MySQL Replication
	  • SNMP Start
	  • SNMP Stop
	  • SNMP Restart
	  • System Snapshot
	  • Generate Key
	• Database Backup and Restore
	  • Database Backup
	  • Delete Backup
	  • Restore
	  • Restore From Remote File
	• Space Troubleshooting
	  • Log Configuration
	• Applications
	  • Junos Space Store
	  • Modify Application Settings	

Table 126: Predefined Roles (R through Z) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace
	• Refresh Search Index • Manage Services • Uninstall Application • Upgrade Application • Add Application • Upgrade Platform • Licenses • Import License • Tags • Create Public Tag • Modify Public Tag • Delete Public Tags • Delete Private Tags • Make Tag Public • Mark as Favorite • Unmark as Favorite • Export Tags • Filter Management • Save Filter • Modify Filter • Delete Filter • DMI Schemas • Set as Default Schema • View Missing Schemas • View/Delete Unused Schemas • Delete Unused Schemas • Update Schema • Authentication Servers • Platform Certificate • CA/CRL Certificates • SMTP Servers	

Table 126: Predefined Roles (R through Z) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace

	• Audit Log Forwarding
	  ◦ Create Audit Log Forwarding Criterion
	  ◦ Modify Audit Log Forwarding Criterion
	  ◦ Delete Audit Log Forwarding Criterion
	  ◦ Enable Audit Log Forwarding Criterion
	• Email Listeners
	• Proxy Server
	• Purging Policy
	  ◦ Modify Purging Policy
	  ◦ Edit Purging Policy
	  ◦ Set Policy Status	

Tag Administrator	• Tags
	  ◦ Modify Public Tag
	  ◦ Delete Public Tags
	  ◦ Delete Private Tags
	  ◦ Mark as Favorite
	  ◦ Unmark as Favorite
	  ◦ Export Tags
	  ◦ Make Tag Public
	  ◦ Create Public Tag
		Network Management Platform > Administration > Tags

Template Design Manager	• Device Templates
	  ◦ Definitions
	  ◦ Create Template Definition
	  ◦ Manage CSV Files
	  ◦ Modify Template Definition
	  ◦ Clone Template Definition
	  ◦ Publish Template Definition
	  ◦ Unpublish Template Definition
	  ◦ Delete Template Definition
	  ◦ Export Template Definition
	  ◦ Import Template Definition
	  ◦ Assign Definition to Domain
		Network Management Platform > Device Templates > Definitions

Table 126: Predefined Roles (R through Z) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace

Template Manager	• Devices
	  ◦ Create Quick Template
	• Device Templates
	  ◦ Templates
	  ▪ Create Quick Template
	  ▪ Create Template from Definition
	  ▪ View Template Details
	  ▪ Modify Quick Template
	  ▪ Modify Template
	  ▪ Delete Template
	  ▪ Audit Template Configuration
	  ▪ Compare Template Against Device
	  ▪ Clone Template
	  ▪ Undeploy Template
	  ▪ View Template Association
	  ▪ Export Quick Template
	  ▪ Import Quick Template
	  ▪ Assign/Deploy Template
	  ▫ Assign Template
	  ▫ Deploy Template
	  ▪ Assign Template to Domain
	  ▪ Unassign from Device
	  ◦ Manage CSV Files
		Network Management Platform > Devices
		
		Network Management Platform > Device Templates > Templates

Table 126: Predefined Roles (R through Z) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace

User Administrator	• Role Based Access Control
	  ◦ User Accounts
	  ▪ Create User
	  ▪ Modify User
	  ▪ Delete Users
	  ▪ Disable Users
	  ▪ Enable Users
	  ▪ Unlock Users
	  ▪ Clear Local Passwords
	  ◦ User Groups
	  ▪ Create User Group
	  ▪ Modify User Group
	  ▪ Delete User Groups
	  ▪ Assign Group to Users
	  ◦ Roles
	  ▪ Create Role
	  ▪ Modify Role
	  ▪ Clone Role
	  ▪ Delete Roles
	  ▪ Export Roles
	  ▪ Import Roles
	  ◦ Remote Profiles
	  ▪ Create Remote Profile
	  ▪ Modify Remote Profile
	  ▪ Delete Remote Profiles
	  ◦ API Access Profiles
	  ▪ View API Access Profile Detail
	  ▪ Create API Access Profile
	  ▪ Modify API Access Profile
	  ▪ Delete API Access Profiles
	  ◦ User Sessions
	  ▪ Terminate User Session
		Network Management Platform > Role Based Access Control

Table 126: Predefined Roles (R through Z) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace

Xpath and Regex Manager	• CLI Configlets
	  • Xpath and Regex
	  • Create Xpath / Regex
	  • Modify Xpath / Regex
	  • Delete Xpath / Regex
	  • Assign XPath / Regex to Domain
		Network Management Platform > CLI Configlets

RELATED DOCUMENTATION

- Role-Based Access Control Overview | **995**
- Configuring Users to Manage Objects in Junos Space Overview | **1033**
- Managing Roles | **1024**
- Creating a User-Defined Role | **1022**
- Modifying User-Defined Roles | **1026**
- Deleting User-Defined Roles | **1027**
- Creating Users in Junos Space Network Management Platform | **1035**
- Viewing Users | **1054**
- Viewing User Statistics | **1068**

Creating a User-Defined Role

Junos Space Network Management Platform provides read-only predefined roles—that is, Super Administrator or User Administrator—that you can use to create users to perform tasks that their roles permit. You can also create read/write user-defined roles that determine user responsibilities and access privileges for your network. You can modify and delete only user-defined roles that you create. You cannot modify or delete predefined roles.

To create a user-defined role:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **Roles**.

   The Roles page appears.

2. Click the **Create Role** icon on the menu bar.

   The Create Role page appears, allowing you to select workspaces and associated tasks from all deployed applications.

3. In the **Title** text box, type a user-defined role name.

   The role title cannot exceed 32 characters. The title can contain letters and numbers and can include a hyphen (-), underscore (_), or period (.). Also, the title cannot start with a space.

4. In the **Description** text box, type a user-defined role description.

   The role description cannot exceed 256 characters. The description can contain letters and numbers and can include a hyphen (-), underscore (_), period (.), or comma (,).

5. Select an application workspace from the application selection ribbon.

   Mouse over an application workspace icon to view the application and workspace name. You can select one or more workspaces for each user-defined role. An expandable and collapsible tree of associated tasks appears below the selection ribbon.

6. From the task tree, select the specific tasks that you want for the user-defined role. All application workspace tasks are selected by default in the task tree.

   Only the application workspace node that is currently being edited is expanded in the Task Summary pane; previously selected workspace nodes are collapsed. You can expand other workspace nodes manually.

   Selecting the top node or workspace selects or deselects the whole task tree. Selecting any task node automatically selects all tasks under the task node. Selecting any task node automatically selects its parent and grandparent.

   Only the currently active task tree appears in the Task Summary pane.

7. Click **Create**.

   The user-defined role is created, is saved, and appears on the Roles inventory page.

   Scroll or search to view it.

NOTE: You cannot create or save a user-defined role when the workspace tasks are not selected. Junos Space displays the following error message:

Task tree selection cannot be empty.

Creation of a role generates an audit log entry.

RELATED DOCUMENTATION

- Predefined Roles Overview | **999**
- Managing Roles | **1024**
- Modifying User-Defined Roles | **1026**
- Deleting User-Defined Roles | **1027**
- Creating Users in Junos Space Network Management Platform | **1035**

Managing Roles

IN THIS SECTION

- Viewing User Role Details | **1024**
- Managing Predefined and User-Defined Roles | **1025**

A role is a specific set of tasks that can be assigned to users in Junos Space Network Management Platform. Junos Space Platform provides predefined roles, as well as the provision to create user-defined roles, that can both be assigned to users. A Super Administrator or User Administrator can view all predefined and user-defined roles on the **Role Based Access Control** > **Roles** inventory page and create new user-defined roles if required.

Viewing User Role Details

The **Roles** inventory page displays all predefined and user-defined roles in tabular format.

Roles are listed in the table in ascending alphabetical order. The columns indicate the role title, type (that is, predefined or custom), description, and tasks assigned. You can show or hide table columns and sort records in ascending or descending order.

You can search for roles by typing the first letters of the role title in the search box. Role titles starting with the first letters you type are listed.

To view a user role detail summary:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **Roles**.

   The Roles page appears.

2. Double-click a role.

   The Role Detail Summary page that appears displays the workspace and workspace tasks assigned to that role.

3. Click the expander button **+** adjacent to the workspaces to view subtasks.

4. Click **OK** on the Role Detail Summary page to exit this page.

   You are returned to the Roles page.

Managing Predefined and User-Defined Roles

You can manage predefined and user-defined roles by selecting a task from the Actions menu or the shortcut menu that is displayed when you right-click a role, or by clicking the icons at the top of the Roles page. You can perform the **Modify Role** and **Delete Roles** actions only on user-defined roles. You cannot manipulate read-only predefined roles. To perform an action, you must first select the role.

You can perform one or more of the following actions by using the Roles page:

- **View Role Details**—View details about the selected role.
- **Modify Role**—For selected user-defined roles, modify the description, application workspaces, and tasks assigned to the role. You cannot modify predefined roles. For more information, see “Modifying User-Defined Roles” on page 1026.
- **Delete Roles**—Delete the selected user-defined roles. You cannot delete predefined roles. For more information, see “Deleting User-Defined Roles” on page 1027.
- **Clone Roles**—Clone the selected user-defined or predefined roles. For more information, see “Cloning Predefined and User-Defined Roles” on page 1028.
- **Tag It**—Tag one or more selected inventory objects. For more information, see “Tagging an Object” on page 1526.

- **View Tags**—View a list of tags applied to a selected inventory object. For more information, see "Viewing Tags for a Managed Object" on page 1532.
- **Untag It**—Remove tags that are applied to inventory objects. For more information, see "Untagging Objects" on page 1527.
- **Delete Private Tags**—Delete tags that you created.
- **Clear All Selections**—Clear all role selections you made on the Roles inventory page.
- **Display Quick View**—View a small window summarizing data about the selected object.

RELATED DOCUMENTATION

Role-Based Access Control Overview | **995**

Predefined Roles Overview | **999**

Creating Users in Junos Space Network Management Platform | **1035**

Creating a User-Defined Role | **1022**

Modifying User-Defined Roles | **1026**

Deleting User-Defined Roles | **1027**

Modifying User-Defined Roles

As a Super Administrator or User Administrator, you can modify user-defined roles. You can modify the description, application workspace, and the selected tasks of a user-defined role. You cannot modify the title. If you modify the role assigned to a user when the user is logged in, the change in the role becomes effective only when the user initiates another session. Changes in a role do not impact existing user sessions. This is applicable for both API and GUI user sessions.

To modify a user-defined role:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control >Roles**.

   The Roles inventory page appears displaying all existing predefined and user-defined roles.

2. Select the user-defined role you want to modify.

3. Click the **Modify Role** icon.

4. Modify the part of the user-defined role that you want: description, application workspace, or tasks.

The role description cannot exceed 256 characters. The description can contain letters and numbers and can include a hyphen (-), underscore (_), period (.), or comma (,).

5. Click **Modify**.

   The modified user-defined role is updated on the Roles inventory page.

Modification of a role generates an audit log entry.

RELATED DOCUMENTATION

- Predefined Roles Overview | **999**
- Creating Users in Junos Space Network Management Platform | **1035**
- Managing Roles | **1024**
- Roles Overview | **998**
- Creating a User-Defined Role | **1022**
- Deleting User-Defined Roles | **1027**

Deleting User-Defined Roles

As a Super Administrator or User Administrator, you can delete user-defined roles from the **Roles** inventory page only if they are not assigned to other users.

> **NOTE:** You cannot delete predefined roles.

To delete a user-defined role:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **Roles**.

   The Roles inventory page appears displaying all existing predefined and user-defined roles.

2. Select the user-defined roles that you want to delete.

3. Click the **Delete Roles** icon.

The Delete Roles dialog box appears asking you for confirmation.

4. Click **Delete**.

   The role is deleted from the Roles inventory page.

> **NOTE:** If the role is assigned to other Junos Space Network Management Platform users, you cannot delete the role. Junos Space displays an error message similar to: **Role "test-role-1" cannot be deleted because it is referenced by users: test-role-user (test role user).**

Deletion of roles generates an audit log entry.

RELATED DOCUMENTATION

- Predefined Roles Overview | **999**
- Managing Roles | **1024**
- Creating a User-Defined Role | **1022**
- Roles Overview | **998**
- Modifying User-Defined Roles | **1026**
- Creating Users in Junos Space Network Management Platform | **1035**

Cloning Predefined and User-Defined Roles

As a Super Administrator or User Administrator, you can clone predefined and user-defined (custom) roles from the **Roles** inventory page. When you clone a role, you are creating a copy of a role, renaming it, and editing it to suit your requirements. This approach is a quick way to create a new role without having to create it from scratch.

To create a role that is similar to a predefined role, clone the predefined role and make suitable changes to the clone.

> **NOTE:** Junos Space Network Management Platform does not allow you to modify predefined roles.

The clone is not applied to any users, by default. The Super Administrator, or the User Administrator with permissions to assign roles to a user can assign this role to users and remote profiles.

To clone a predefined and user-defined role:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control >Roles**.

   The Roles inventory page appears displaying all existing predefined and user-defined roles.

2. Right-click the predefined or user-defined role that you want to clone and select **Clone Role**. Alternatively, select a role, then select **Clone Role** from the Actions menu.

   The Clone Role page appears with the specifications of the original role.

   > **NOTE:** If **Clone Role** is disabled, ensure that you have the **Clone Role** permission and that you have not selected more than one role.

3. In the **Title** text box, enter the name of the clone.

   The name cannot start with a space or exceed 32 characters; allowable characters include letters, numbers, dash (–), underscore (_), and period (.). You cannot have two roles with the same name.

4. (Optional) In the **Description** field, enter or modify the description of the clone.

   The description cannot exceed 256 characters. The description can contain letters and numbers and can include a hyphen (-), underscore (_), period (.), or comma (,).

5. (Optional) Select the application workspaces and associated tasks for the cloned role by selecting the check box corresponding to the workspace or task.

   For more information about selecting workspaces and tasks, see the "Creating a User-Defined Role" on page 1022 topic.

6. Click **Clone**.

   A new role is created and displayed on the Roles inventory page. On this page, click the **View Detail** link to view the tasks assigned to this role.

After a role is cloned, you can perform various actions on this role such as modifying its details, deleting the role, and so on. For more information, see the "Managing Roles" on page 1024 topic.

RELATED DOCUMENTATION

Roles Overview | 998

Managing Roles | 1024

Exporting User-Defined Roles from Junos Space Network Management Platform

You can export user-defined roles from the Junos Space Network Management Platform database and download them to your local computer.

> **NOTE:** You cannot export predefined roles from Junos Space Platform.

To export user-defined roles from Junos Space Platform:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > Roles**.

   The Roles page that appears displays all roles that currently exist in the Junos Space Platform database.

2. Right-click the user-defined roles that you want to export and select **Export Roles**.

   The Export Roles dialog box that appears displays the roles that you selected.

   > **NOTE:** If you select a predefined role, the **Export Roles** menu item appears dimmed.

3. Click **Export** and save the XML file to your local computer.

   The Export Roles Job Status dialog box displays the status of the export roles job.

   Close the dialog box to return to the Roles page.

RELATED DOCUMENTATION

Managing Roles | 1024

Modifying User-Defined Roles | 1026

Importing Roles to Junos Space Network Management Platform | 1031

Importing Roles to Junos Space Network Management Platform

Using Junos Space Network Management Platform, you can import user-defined roles to the Junos Space Platform database. Role definitions stored as XML files can be imported into Junos Space Platform from your computer. We recommend that you view the sample XML file by using the link provided in the Roles dialog box before you import roles for the first time. Multiple XML files can be imported one by one.

NOTE: You cannot import a role in the following scenarios:

- The name of the role that you entered in the XML file exists in the Junos Space Platform database.
- You did not enter details for mandatory tags in the XML file.

To import roles to Junos Space Platform:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > Roles**.

   The Roles page that appears displays all roles that currently exist in the Junos Space Platform database.

2. Click the Import roles icon on the toolbar.

   The Import Roles page is displayed.

3. (Optional) To view a sample XML file, click the **View Sample XML** link.

   Refer to this file for the details required to import roles to Junos Space Platform.

4. Click **Browse** and select the XML file from your local computer.

5. Click **Import**.

   A progress bar indicates the status of the import roles job. If the roles are imported successfully, the Import Role Information dialog box appears displaying details of the import roles job. If the roles are not imported, an error message is displayed.

Click **OK** to return to the Roles page.

RELATED DOCUMENTATION

Managing Roles | 1024

Modifying User-Defined Roles | 1026

CHAPTER 60

User Accounts

IN THIS CHAPTER

- Configuring Users to Manage Objects in Junos Space Overview | **1033**
- Creating Users in Junos Space Network Management Platform | **1035**
- Modifying a User | **1044**
- Deleting Users | **1050**
- Disabling and Enabling Users | **1051**
- Unlocking Users | **1053**
- Viewing Users | **1054**
- Exporting User Accounts from Junos Space Network Management Platform | **1061**
- Changing Your Password on Junos Space | **1065**
- Clearing User Local Passwords | **1067**
- Viewing User Statistics | **1068**

Configuring Users to Manage Objects in Junos Space Overview

Junos Space Network Management Platform is shipped with a Super Administrator privilege level that provides full access to the Junos Space system. When you first log in to Junos Space Network Management Platform as default Super Administrator, you can perform all tasks and access all Junos Space system resources. Super Administrator can create users and assign roles to those users to specify which workspaces and system resources the users can access and manage, and which tasks the users can perform within each workspace.

After you first set up Junos Space Network Management Platform, you can disable the default Super Administrator user ID, if necessary. However, before doing so, you should first create another user with Super Administrator privileges.

To access and manage Junos Space system resources, a user must be assigned at least one role. A *role* defines the tasks (create, modify, delete) that can be performed on the objects (devices, users, roles, configlets, scripts, services, customers) that Junos Space Network Management Platform manages. For more information about roles, see “Roles Overview” on page 998.

Users receive permission to perform tasks only through the roles that they are assigned. In most cases, a single role assignment enables a user to view and to perform tasks on the objects within a workspace. For example, a user assigned the Device Manager role can discover devices, resynchronize devices, view the physical inventory and interfaces for devices, and delete managed devices. A user that is assigned the User Administrator role can create, modify, and delete other users in Junos Space, and assign and remove roles.

If you modify a role assigned to a user when the user is logged in, the change becomes effective only when the user initiates another session. Changes in a role do not impact existing user sessions. This is applicable for both API and GUI user sessions.

Typically, a role contains one or more task groups. A *task group* provides a mechanism for grouping a set of related tasks that can be performed on a specific object.

> **NOTE:** You can assign multiple roles to a single user, and multiple users can be assigned the same role.

User-Specific Idle Timeout

From Junos Space Platform Release 17.1R1 onward, you can specify user-specific idle time out — a period of inactivity after which the user session expires — values when you create or modify a user account.

> **NOTE:** Only users who have super administrator or user administrator roles, or have permissions to create or modify user accounts can configure user accounts.

You can specify a value in the range of 0 through 480 minutes in the **Automatic logout after inactivity (minutes)** field of the Create User page or the Modify User page. If you set the idle time out value to 0, the user session never expires. By default, the user-specific idle time out value is set to the **Automatic logout after inactivity (minutes)** value configured in the User Settings section of the **Administration** > **Application Settings** page.

If a user has multiple GUI sessions open, only those sessions that exceed the value configured for **Automatic logout after inactivity (minutes)** expire.

If you modify the **Automatic logout after inactivity (minutes)** setting for a user account (**Modify User Page**) while the user has GUI sessions open, those sessions continue to use the previously-configured value for the idle time out. The new value applies only to those sessions that the user opens after you modify the idle time out settings.

Release History Table

Release	Description
17.1	From Junos Space Platform Release 17.1R1 onward, you can specify user-specific idle time out — a period of inactivity after which the user session expires — values when you create or modify a user account.

RELATED DOCUMENTATION

- Role-Based Access Control Overview | **995**
- Creating Users in Junos Space Network Management Platform | **1035**
- Viewing Users | **1054**
- Viewing User Statistics | **1068**

Creating Users in Junos Space Network Management Platform

You create user accounts in Junos Space Network Management Platform, which are stored in the Junos Space Platform database. You can then assign different roles to the users associated with these user accounts, depending on the network management tasks the users are required to perform in your network.

When a user attempts to log in to Junos Space Platform, the user is allowed to log in only if authenticated. Junos Space Platform supports credentials-based user authentication and certificate-based user authentication. For more information about user authentication, see "Role-Based Access Control Overview" on page 995.

For credentials-based user authentication, each user account must include:

- Login ID
- Password
- First name
- Last name
- Roles, which determine the tasks that a user can perform within the applications and workspaces
- Domains within which the user can operate

For certificate-based user authentication, each user account must include:

- Login ID
- First name

- Last name
- X.509 certificate file
- Roles, which determine the tasks that a user can perform within the applications and workspaces
- Domains within which the user can operate

You can perform various tasks including the following from the User Accounts page of the Role-Based Access Control workspace of Junos Space Platform:

- Generate user accounts with temporary passwords and set an expiry duration of up to 10,000 hours.
- Set the number of concurrent UI sessions on a per-user basis.
- Determine which users can access Junos Space through the GUI and which through the API.
- Assign multiple roles and domains to new users.
- Assign roles and domains to existing users.
- Manually enable and disable users and unlock users who are locked out.

You can assign specific roles to a user to specify the tasks and objects (devices, users, services, and so forth) that the user can access and manage. You can assign multiple roles to a single user. You can export user accounts from the Reports workspace. To export user accounts, create a User Account report definition in the Reports workspace. Then generate the report from the report definition and download the report. For more information, see "Exporting User Accounts from Junos Space Network Management Platform" on page 1061. You can also limit the number of user login sessions in Junos Space Platform.

Creating a User

As a Super Administrator or User Administrator, you can create users in Junos Space Platform and assign roles to these users. The roles determine the tasks that the users can perform in Junos Space Platform.

As an administrator, you have the option to assign a temporary or permanent password to a new user or an existing user whose password has expired. Consider the points mentioned in Table 127 before assigning a temporary or regular password to a user.

Table 127: Differences Between Temporary and Regular Passwords

Temporary Password	Regular Password
Users must change their temporary passwords at first login.	Users need not change their passwords at first login.

Table 127: Differences Between Temporary and Regular Passwords *(continued)*

Temporary Password	Regular Password
When temporary passwords expire, users cannot access the Junos Space server. To access the Junos Space server, users need to use the new passwords that the administrator has generated and shared with them. Users cannot change their passwords on their own.	When regular passwords expire, users can change their passwords on their own after logging in to the Junos Space server.
Password expiry time is configured at the user level. By default, temporary passwords expire after 24 hours.	Password expiry time is configured at the global level from the Administration workspace. This expiry time applies to all users with regular passwords. For more information about configuring parameters related to regular passwords, see "Modifying Junos Space Network Management Platform Settings" on page 1346.

To create a user:

1. On the Junos Space Platform UI, select **Role Based Access Control** > **User Accounts**.

   The User Accounts page is displayed.

2. Click the **Create User** icon on the toolbar above the application data to display the Create User page.

   The Create User page is displayed. This page displays the General area on the left of the page and the Create User area on the right of the page.

   > **NOTE:** We recommend that you mouse over the blue icons on this page to know more about the fields next to which they are displayed.

3. In the **Login ID** field, enter a login ID for the new Junos Space user.

   This can be an e-mail address. If it is, it is not mandatory that the login ID matches the e-mail address entered in the Email field. The login ID cannot exceed 128 characters. Permitted characters include hyphen (-), underscore (_), letters and numbers, as well as @ and period (.). You cannot have two users with the same login ID.

> **NOTE:** You cannot enter **admin** as the login ID. If you enter **admin** as the login ID, the following error message is displayed:
> **Username admin is reserved in Space. Please do not create user with username: admin.**

4. (Optional) Select the **Generate a temporary password** check box if you want to generate a temporary password for the user. Generation of temporary passwords is supported only for local authentication mode. It is not supported for remote-local authentication or remote authentication modes.

   As an administrator, you may want to generate a random password for a new user or when the password expires for an existing user. Users must change their temporary passwords when they log in for the first time. Users with temporary passwords are not allowed to use any of the features in Junos Space Platform unless they replace their temporary passwords with new passwords.

   When you generate a temporary password for a user, consider configuring the following fields related to the temporary password:

   - **Temporary password will expire after**—Specify the duration after which the temporary password expires. The user must log in to Junos Space within this duration and change the temporary password. Otherwise, after the expiry of the password, the user is not allowed to log in. When the temporary password expires, Junos Space displays the following message:
     Your password has expired.
     Please contact your administrator.

     The user must request the administrator for a new password.

     By default, the temporary passwords expire after 24 hours of their generation. The administrator can enter a value from 1 through 10,000 hours.
   - **Temporary Password**—Displays the temporary password generated by the Junos Space server. To generate another password, click **Generate** next to this field. The new generated password is displayed in this field.
   - **Email password to user**—Select this check box to e-mail the generated temporary password to the user. This check box is disabled if the SMTP server is not configured.

     If the e-mail does not reach the user or the password is lost, the administrator needs to generate a new temporary password. There is no option to resend the old temporary password.

TIP:

For the Junos Space server to automatically send the temporary password and expiry date by e-mail to the user, ensure that you configure:

- The e-mail ID of the user in the **Email** field on the Create User page (the page that you are currently in)
- The SMTP server that receives the e-mail from the Junos Space server and routes it to the intended recipient

  You must configure the SMTP server on the **Administration** > **SMTP Servers** inventory landing page. After configuring the SMTP server, test the connection between the Junos Space server and the SMTP server to ensure that communication between the servers is established. For more information about SMTP server configuration and how to test the configuration, see "Adding an SMTP Server" on page 1478 and "Managing SMTP Servers" on page 1477.

5. In the **Password** field, enter the password.

   This field is disabled if you have chosen to generate a temporary password.

   All passwords in Junos Space Platform are case-sensitive. For information about configuring password rules, see "Modifying Junos Space Network Management Platform Settings" on page 1346.

   The password strength indicator checks and displays the efficiency of the password that you entered.

   NOTE: You cannot proceed to the next step if the password strength indicator shows that the password is weak.

6. In the **Confirm Password** field, reenter the password to confirm the password.

   This field is disabled if you have chosen to generate a temporary password.

7. In the **First Name** field, enter the user's first name.

   The name cannot exceed 32 alphanumeric characters.

8. In the **Last Name** field, enter the user's last name.

   The name cannot exceed 32 alphanumeric characters.

9. (Optional) In the **Email** field, enter the user's e-mail address.

You must enter an e-mail address in this field if you have opted to e-mail the temporary password to a user by selecting the **Email password to user** check box.

This need not be the same as the login ID if the login ID is an e-mail address.

Ensure that the e-mail ID that you enter is valid and uses the format *user@domain*.

10. (Optional)To set a user-specific limit for the maximum number of concurrent UI sessions that are allowed for the user, clear the **Use global settings** check box.

    By default, this check box is selected and the user is allowed five concurrent sessions. This limit is displayed in the **Maximum concurrent UI sessions** field just below this check box. For more information about configuring concurrent UI sessions limits, see "Limiting User Sessions in Junos Space" on page 1108.

    In the **Maximum concurrent UI sessions** field, which becomes active when you clear the **Use global settings** check box, enter the maximum number of concurrent UI sessions that are allowed for this user. The default value for this field is 5.

    You can enter a value from 0 through 999.

    > **NOTE:** If you enter 0 (zero), there is no restriction on the number of concurrent UI sessions allowed for the user. However, the performance of the Junos Space setup may be affected if you allow many users with an unrestricted number of concurrent UI sessions.

11. (Optional) To set a user-specific value for the **Automatic Logout after Inactivity** setting, clear the **Use global settings** check box.

    > **NOTE:** You can configure user-specific idle time out from Release 17.1R1 onward.

    By default, this check box is selected and the value you configured for the **Automatic logout after inactivity (minutes)** field under User Settings of the Modify Network Management Platform page (**Administration** > **Applications** > **Modify Application Settings**) is applied to the user.

    In the **Automatic Logout after Inactivity** field, which becomes active when you clear the **Use global settings** check box, enter the idle time out value in minutes. An idle time out value denotes a period of inactivity after which the user session expires. You can enter a value in the range of 0 through 480 minutes. If you set the value to 0, the user session never expires.

12. (Optional) In the **Image File** field, upload the user's photo ID from your local file system.

13. The fields displayed depend on the mode of authentication chosen for your Junos Space setup. If you enabled complete certificate-based authentication, the X509 Cert File field is displayed. If you enabled password-based authentication or parameter-based authentication, the X.509 Certificate area is displayed with text boxes to enter values for the parameters.

    - If you enabled complete certificate-based authentication:

        i. Click **Browse** adjacent to the X509 Cert File field to select the X.509 certificate file from your local computer.

        You can upload certificate file formats with the following extensions: **.der**, **.cer**, and **.crt**. Junos Space Platform uploads and saves the certificate file for the user.

        ii. Click **Upload**.

        If you upload a certificate, the user is authenticated on the basis of the complete X.509 certificate. For more information about certificate-based user authentication, see "Certificate Management Overview" on page 1426.

    - If you enabled password-based authentication or parameter-based authentication:

        i. In the X.509 Certificate area, enter the values for the parameters.

        A maximum of four X.509 parameters are displayed. For example, the e-mail address of the user or the serial number of the client certificate.

        You must enter a unique value for every parameter for every user. The X.509 certificate parameters are authenticated only during parameter-based authentication.

14. (Optional) At this point, you can click **Finish** to create a user without assigning roles. You can assign roles later.

15. To assign roles, click **Next**

    The Role Assignment page that appears displays the Available and Selected list boxes. All predefined roles are displayed in the Available list box by default.

16. (Optional) To assign the roles of an existing user to the new user, select the **Use Same Roles Assigned to** check box and enter the name of the existing user and click the Search icon.

    All roles assigned to the existing user are displayed in the Available list box. You can modify the new user's role assignments by adding roles to or removing roles from the Selected list box.

- To select the existing user whose privileges you want to assign to the new user, enter one or more characters of the username of the existing user in the Search field to find and select the username.

  The roles assigned to the existing user are displayed in the Selected list box. You can modify the new user's role assignments by adding roles to or removing roles from the Selected list box.

17. (Optional) Select the **GUI Access** or **API Access** check box depending on the type of access you want to allow for the user.

    By default, the user can access both the GUI or API. Select at least one access type to successfully create a user.

18. Select whether the user can view all jobs on Junos Space Platform or only those jobs that the user has selected.

    By default, the View User's Own Job Only option button is selected. If you want the user to view all jobs, select the **View All Jobs** option button.

    NOTE: Users with the Super Administrator or Job Administrator role can view jobs initiated by all users. You cannot modify this privilege in Junos Space Platform. For a new user with the Super Administrator or Job Administrator role, the **View All Jobs** option button is selected by default and the Job Management View area appears dimmed.

    NOTE: If you are upgrading from previous Junos Space Platform releases, the users who are not assigned the Super Administrator or Job Administrator role in the previous release can view only their own jobs on the Job Management page. They cannot view jobs initiated by other users.

19. To associate an API Access Profile to a user to execute RPC commands safely on the device, select the API Access Profile from the **Device command Access via API** drop-down list.

    By default, the **Disallow all exec RPCs** option button is selected.

    For more information about creating API Access Profiles, see "Creating an API Access Profile" on page 1102.

20. To select and assign predefined roles for the user:

    a. Select one or more roles from the **Available** list box and click the right arrow.

       The selected roles are displayed in the **Selected** list box.

       You can also double-click a role to move it between lists.

> **NOTE:** When you install a Junos Space application on Junos Space Platform, the predefined roles for these applications are also available for selection. When you want to restrict a user to a specific Junos Space application, ensure that you assign the role that is related to that application to the user.

> **NOTE:** The minimum role required for configuring a user for IBM Systems Director and Junos Space Launch in Context (LiC) is Device Manager.

b. (Optional) Use the left arrow to move roles from the Selected list box back to the Available list box.

c. (Optional) To view the privileges assigned to a role, click the role in the Available or Selected list boxes.

   The privileges assigned to these roles are displayed next to the Selected list box.

21. (Optional) At this point, you can click **Finish** to create a user without assigning domains to the user. You can assign domains later.

22. To assign domains to the user, click **Next**.

    The Domain Assignment page is displayed. This page displays the domains in a hierarchal tree structure in the Available Domains area.

23. (Optional) To assign domains that are already assigned to an existing user to the new user, select the **Use Same Roles Assigned to** check box, enter the name of the existing user, and click the Search icon.

    All domains assigned to the existing user are displayed in the Available Domains area.

    - To select the existing user whose domain privileges you want to assign to the new user, enter one or more characters of the username of the existing user in the Search field to find and select the username.

      The Available Domains area displays only domains assigned to the existing user.

24. Select the domains that you want to assign to the new user.

    You can select multiple domains at the same hierarchy level.

> **NOTE:** If you do not assign a domain to the user, the Global domain is assigned to the user by default.

25. Click **Finish**.

The new user is created in the Junos Space Platform database. You are returned to the User Accounts page.

Release History Table

Release	Description
17.1R1	You can configure user-specific idle time out from Release 17.1R1 onward.

RELATED DOCUMENTATION

- Configuring Users to Manage Objects in Junos Space Overview | **1033**
- Predefined Roles Overview | **999**
- Changing Your Password on Junos Space | **177**
- Modifying a User | **1044**
- Deleting Users | **1050**
- Viewing Users | **1054**

Modifying a User

As a Super Administrator or User Administrator, you can modify any user account in Junos Space Network Management Platform. The only attribute that cannot be modified is the login ID.

The Modify User page has three areas—General, Role Assignment, and Domain Assignment—in which user information is grouped accordingly. Each user account can have multiple roles and a role can be associated with multiple users.

To modify an existing user account:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **User Accounts**.

   The User Accounts inventory page appears.

2. From the inventory page, select the user account that you want to modify. For instructions on filtering and sorting, see "Viewing Users" on page 1054.

   You can modify only one user account at a time.

3. From the menu bar above the table, click the **Modify User** icon (the pencil icon).

The **Modify User** page appears, displaying the General area by default, with the existing account information for that user.

4. You can change any of the information in the General area except the login ID.

   - To generate a temporary password, select the **Generate a temporary password** check box. You generate passwords for new users or existing users whose passwords have expired. Generation of temporary passwords is supported only for local authentication mode. It is not supported for remote-local authentication or remote authentication modes.

     To generate a temporary password, configure the following fields:

     - **Temporary password will expire after**—Specify the duration after which the temporary password expires. The user must log in to Junos Space within this duration and change the temporary password. Otherwise, after the expiry of the password, the user is not allowed to log in. When the temporary password expires, Junos Space displays the following message:
       Your password has expired.
       Please contact your administrator.

       The user must request the administrator for a new password.

       By default, the temporary passwords expire after 24 hours of its generation. The administrator can enter a value from 1 through 10,000.

     - **Temporary Password**—View the temporary password generated by the Junos Space server. To generate another password, click **Generate** next to this field. The new generated password is displayed in this field.

     - **Email password to user**—Select this check box to e-mail the generated temporary password to the user. This check box is disabled if the SMTP server is not configured.

       If the e-mail does not reach the user or the password is lost, the administrator needs to generate a new temporary password. There is no option to resend the old temporary password.

TIP:

For the Junos Space server to automatically send the temporary password and expiry date by e-mail to the user, ensure that you configure:

- The e-mail ID of the user in the **Email** field on the Create user page (the page that you are currently in)
- The SMTP server that receives the e-mail from the Junos Space server and routes it to the intended recipient

  You configure the SMTP server on the **Administration** > **SMTP Servers** inventory landing page. After configuring the SMTP server, test the connection between the Junos Space server and the SMTP server to ensure that communication between the servers is established. For more information about SMTP server configuration and how to test the configuration, see "Adding an SMTP Server" on page 1478 and "Managing SMTP Servers" on page 1477.

- To view the rules governing password creation, mouse over the information icon, the small blue *i* to the right of the Password field. To configure the password rules, see "Modifying Junos Space Network Management Platform Settings" on page 1346.
- To change the username, enter a new name in the **First Name** and **Last Name** fields.
- To change the e-mail account, enter a new e-mail address in the **Email** field.
- To change the maximum number of concurrent UI sessions for the user:

  a. If the **Use global settings** check box is selected, clear it.

     The **Maximum concurrent UI sessions** field becomes active.

  b. Enter the number of sessions in the **Maximum concurrent UI sessions** field.

     You can enter a value from 0 through 999. Entering 0 (zero) means that there is no restriction on the number of concurrent UI sessions allowed for the user. However, the system performance may be degraded if you allow unlimited sessions.

  c. If you want to replace a user-specific value with the global value, select the **Use global settings** check box.

- To change the idle time out — a period of inactivity after which the user session expires — setting for the user:

NOTE: You can configure user-specific idle time out from Release 17.1R1 onward.

a. If the **Use global settings** check box next to **Automatic logout after inactivity** is selected, clear it.

   The **Automatic logout after inactivity** field becomes active.

b. Enter the number of minutes the user session can remain inactive before the session expires because of inactivity. You can enter a value in the range of 0 through 480. If you set the value to 0 (zero), the user session never expires.

c. If you want to replace a user-specific value with the global value, select the **Use global settings** check box.

   If you select the **Use global settings** check box, the value you configured for the **Automatic logout after inactivity (minutes)** field under User Settings of the Modify Network Management Platform page (**Administration** > **Applications** > **Modify Application Settings**) is applied to the user.

- (Optional) To upload an image file from your local file system:

  a. Use the **Browse** button adjacent to the **Image File** field to locate the new user photo ID file.

     You can upload BMP, GIF, JPG, and PNG image file formats.

  b. Click **Upload**.

     Junos Space Network Management Platform updates the photo ID file for the user account.

- (Optional) To upload the user's X.509 certificate file from your local file system:

  a. Use the **Browse** button adjacent to the **X509 Cert File** field to locate the user's X.509 certificate file on your local system.

     You can upload certificate file formats with the following extensions: .der, .cer, and .crt.

  b. Click **Upload**.

     Junos Space Network Management Platform uploads and saves the certificate file for the user account. If you upload a certificate, the user is authenticated based on the certificate and not the user credentials (username and password). For more information about certificate-based user authentication, see "Certificate Management Overview" on page 1426.

5. To add or remove role assignments, click **Role Assignment** on the upper right of the Modify User page or click **Next** on the bottom right of the Modify User page.

> **TIP:** When you install various applications in Junos Space, predefined roles for each of these applications are made available to you, and you can view these roles from the Role Based Access Control workspace. So when you want to restrict a user to a specific application, make sure that you assign the role specific to that application while creating or modifying the user.

- To add role assignments, select one or more roles from the Available Roles column and click the right arrow to move the roles to the Selected Roles column.
- To remove role assignments, select one or more roles from the Selected Roles column and click the left arrow to move the roles to the Available Roles column.
- Select or clear the **GUI Access** and **API Access** check boxes depending on the type of access you want to allow for the user.
- Select **View All Jobs** or **View User's Own Jobs Only** to enable users to view jobs triggered by all users or view only their own jobs. By default, a user with the Super Administrator or Job Administrator role can view jobs of all users and you cannot modify this configuration.

6. To add, remove, or change domain assignments, click **Domain Assignment** on the upper right of the Modify User page, or click **Next** on the lower right of the Modify User page.
   - Select the domains to which the new user must be assigned. By default, the user is assigned to the **Global** domain.

     > **NOTE:** The user must be assigned to at least one domain.

7. Click **Finish** at the bottom of the page to complete the modification.

   Junos Space Network Management Platform updates the user account with the changes you specified. However, a confirmation message appears if you have removed any role; for example, if you removed the Device Script Manager role from a user, a confirmation pop-up is displayed.

   Perform one of the following tasks:

   - Click **No** to ensure that previously scheduled jobs are not affected. Junos Space Platform automatically adds the necessary role (that you removed) to the user ensuring that the user has the permissions to execute the jobs and that the jobs are not affected.
   - Click **Yes** to modify the user role. If you choose this option, scheduled jobs affected by this modification are not executed because this user no longer has access to the workspaces in which the jobs are scheduled. To ensure that the jobs are executed, you must reassign these jobs to another user. For more information, refer to the "Reassigning Jobs" on page 982 topic.

When you remove the role, this user cannot perform any actions on the impacted job on the Job Management page, such as cancel the job, reassign the job, reschedule the job, and so on. The only actions permitted are: the user can tag the job and clear the selection of the job.

NOTE: When a job is executed, Junos Space Platform verifies whether the job owner has the permission to execute the job. If the job owner does not have the necessary permissions, the job is canceled. When you double-click the job, a message indicating that the user does not have the necessary permission to execute the job is displayed.

NOTE: If the **Email password to user** check box is enabled during user modification, then the "Mail user password" job is triggered and an audit entry is made to record this action.

Release History Table

Release	Description
17.1R1	You can configure user-specific idle time out from Release 17.1R1 onward.

RELATED DOCUMENTATION

- Configuring Users to Manage Objects in Junos Space Overview | **1033**
- Creating Users in Junos Space Network Management Platform | **1035**
- Deleting Users | **1050**
- Viewing Users | **1054**

Deleting Users

When a Junos Space Network Management Platform user leaves your organization or no longer needs access to the system, the administrator should delete the existing user account.

To delete one or more users:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **User Accounts**.

   The User Accounts inventory page appears, displaying all user accounts in a table.

2. Select one or more users to delete.

3. From the menu bar above the table, click the **Delete Users** icon.

   The Delete Users confirmation dialog box appears displaying only users with no pending jobs.

4. Retain the selection of the **Exclude users who have jobs in scheduled or inprogress state** check box, if you do not want to delete users who have initiated jobs that are in progress or who have scheduled jobs. That is, when you retain the selection of this check box, you delete only users with no pending jobs.

   NOTE: You might notice that some of the users you selected for deletion do not appear in the Delete Users Confirmation dialog box. This is because these local and remote users are assigned to scheduled, in progress, or recurring jobs and are by default excluded from deletion. To delete these users, you need to clear the **Exclude users who have jobs in scheduled or inprogress state** check box. When this check box is cleared, these users appear in the dialog box and are deleted when you click **Delete**. The **Jobs Scheduled/Inprogress** column in the Delete Users Confirmation dialog box displays **Yes** for users who have scheduled jobs or who have initiated jobs that are in progress.

   Before you delete users with pending jobs, reassign these jobs to other active users within the same domain so as to ensure that these jobs are monitored and successfully completed. For example, reassign a recurring database backup job owned by UserA to UserB before deleting UserA. For more information about reassigning jobs, see “Reassigning Jobs” on page 982.

5. Verify the list of users that you want to delete and click **Delete**. This button is disabled if there are no users to delete.

   All selected user accounts that are displayed in the Delete Users Confirmation dialog box are removed from the Junos Space Network Management Platform database and the User Accounts inventory page.

Deleting users generates an audit log entry. The audit log entry records the users that were deleted.

To obtain details from an audit log entry about users who were deleted:

1. On the Junos Space Network Management Platform user interface, select **Audit Logs** > **Audit Log**.

   The Audit Log inventory page appears, displaying all log entries in a table.

2. Filter data in the **Task** column by using the **Delete Users** keyword.

   After filtering, the Audit Log page displays only the audit log entries that were generated when users were deleted.

3. Double-click an audit-log entry.

   The Audit Log Detail page appears. On this page, the **Affected Objects** section displays the list of users who were deleted and the **Affected Object Detail** section displays details about the deleted user.

4. Click **OK** on the Audit Log Detail page to exit this page.

   You are returned to the Audit Log page.

RELATED DOCUMENTATION

Creating Users in Junos Space Network Management Platform | 1035

Modifying a User | 1044

Viewing Users | 1054

Disabling and Enabling Users

From Junos Space Network Management Platform, you can disable a user to prevent the user from logging in to the system. By default, all users are enabled.

NOTE:

- You cannot disable your own user account.
- You cannot disable the **super** user. However, you can disable a user with the Super Administrator role.

You can also configure Junos Space Platform to automatically disable users after a specific period of inactivity. On the **Administration** > **Applications** page, select Network Management Platform and modify

the settings to specify the number of days after which an inactive user is automatically disabled. For more information, see "Modifying Junos Space Network Management Platform Settings" on page 1346.

From the status of the user, which is displayed in the **Status** column on the User Accounts inventory landing page or in the **Status** field on the User Detail Summary page, you can determine whether the user account is enabled or disabled.

When a user whose account is disabled tries to log in to the system, the user sees the message, **This account is disabled**. If the user is active at the time the user account is disabled, the system logs off the user and displays a message indicating that the user account is disabled. In both cases, an audit log entry is automatically generated. The following is a sample audit log entry:
Login Failed. The user is disabled.

To disable or enable one or more users:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > User Accounts**.

   The User Accounts page appears.

2. Select one or more users to disable or enable.

   > **NOTE:** If both the Enable and the Disable actions are unavailable, you have selected a super user.

3. Select **Disable Users** or **Enable Users** from the Actions menu.

   The Disable or Enable Users confirmation dialog box appears, displaying the list of users to whom the selected action will be applied. Users you selected, but who do not appear on the list, will not have the action applied to them. Only those users who are not already in the state to which you want to convert them can be enabled or disabled. If you selected disabled users to disable again, a message appears indicating that the status cannot be changed.

4. Verify the list of users that you want to disable or enable, and click **Disable** or **Enable**, respectively.

   All selected user accounts are disabled or enabled.

When you enable or disable a user, an audit log entry is automatically generated. To view details about users whom you have enabled or disabled from the audit log, double-click the audit log entry. For example, double-click the **Disable Users** audit log entry in the **Task** column. The Audit Log Detail page appears, which displays the users that are disabled. Select a user from the **Affected Objects** section. Details about the user are displayed in the **Affected Object Detail** section to the right of the page.

RELATED DOCUMENTATION

Creating Users in Junos Space Network Management Platform | 1035

Modifying a User | 1044

Viewing Users | 1054

Junos Space Audit Logs Overview | 1115

Unlocking Users

Junos Space Network Management Platform locks out users who enter more than the permitted number of incorrect passwords. If you try to log in to the Junos Space server when your user account is locked out, then you see the message **The account is Locked. You can't Log in.** You can try logging in from another system or request the administrator to unlock your account.

By default, a user is locked out after four unsuccessful login attempts. As an administrator, you can decide after how many unsuccessful login attempts a user should be logged out. You can configure this setting from the Administration workspace. For more information about configuring this setting, see the **No. of unsuccessful attempts before lockout** parameter in "Modifying Junos Space Network Management Platform Settings" on page 1346.

To unlock a user account:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **User Accounts**.

   The User Accounts inventory page appears, displaying all user accounts in a table.

2. Select one or more locked users to unlock.

   > **TIP:** You can identify the locked-out users by the lock icon in the **Locked Out** column on the User Accounts inventory page.

3. Select **Unlock Users** from the Actions menu.

   A confirmation dialog box appears, displaying the users you have selected to unlock.

   If **Unlock Users** is disabled, it means that one or more users that you have selected to unlock is not a locked-out user. Go to step 2 and select only locked-out users to proceed.

4. Click **Unlock** in the confirmation dialog box to unlock the users.

   The selected users are unlocked. These users can log in at the next login attempt.

Unlocking users generates an audit log entry with details about users that were unlocked.

To obtain details from an audit log entry about users who were unlocked:

1. On the Junos Space Network Management Platform user interface, select **Audit Logs** > **Audit Log**.

   The Audit Log inventory page appears, displaying all log entries in a table.

2. Filter data in the **Task** column by using the **Unlock Users** keyword.

   Then the Audit Log page displays only the audit log entries that were generated when users were unlocked.

3. Double-click an audit log entry.

   The Audit Log Detail page appears. On this page, the **Affected Objects** section displays the list of users who were unlocked and the **Affected Object Detail** section displays details about the unlocked user.

4. Click **OK** on the Audit Log Detail page to exit this page.

   You are returned to the Audit Log page.

RELATED DOCUMENTATION

Role-Based Access Control Overview | **995**

Viewing Users

The User Accounts inventory page displays all Junos Space Network Management Platform users who have accounts. To add new users, you must have administrator privileges. To add a new user, see "Creating Users in Junos Space Network Management Platform" on page 1035. Users have Junos Space access based on predefined roles (see "Predefined Roles Overview" on page 999). For more information about how to manipulate inventory page data, see the "Junos Space User Interface Overview" on page 89 topic in the *Junos Space Network Management Platform User Interface Guide*.

To view the inventory of users and their details, select **Role Based Access Control** > **User Accounts**.

The User Accounts page appears.

Users are displayed in a table sorted, by default, by username. Each user occupies a row in the User Accounts table. The table's column headings are User Name, First Name, Last Name, Email, User Type, GUI/API Access, Status, Password Status, and Locked Out.

The status bar at the bottom of the page shows the range of objects that are displayed. For example, you might see *Displaying 1-30 of 113*. In addition, the **Show items** list enables you to select the number of items to display per page: 10, 20, 40, 60, 80, 100, 200.

The following sections describe how you can modify your view to see the user information of interest to you.

- Sorting Columns | **1055**
- Displaying or Hiding Columns | **1055**
- Filtering Users | **1056**
- Viewing User Details | **1057**
- Performing Actions on Users | **1060**

Sorting Columns

The columns in the User Accounts table (that is on the User Accounts inventory landing page) can be arranged in the ascending or descending order.

To sort the contents of a column:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **User Accounts**.

   The User Accounts page appears, displaying the users in tabular format.

2. Click the down arrow to the right of any column heading.

   A list with the following menu options appears:

   - **Sort Ascending**: Select to arrange the contents of the column in ascending order
   - **Sort Descending**: Select to arrange the contents of the column in descending order
   - **Columns**: Select to view the column list from which you can select columns to display
   - **Filters**: Select to enter the filter

3. Select **Sort Ascending** or **Sort Descending**.

   The sequence of objects in the column changes to reflect your choice.

Displaying or Hiding Columns

The columns in the User Accounts table (that is on the User Accounts inventory landing page) can be displayed or hidden as required.

To display or hide a column:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **User Accounts**.

   The User Accounts page appears, displaying the users in tabular format.

2. Click the down arrow to the right of any column heading.

3. Select **Columns**.

   A list with menu options corresponding to all the available column headings appears with a check box next to each heading. The check boxes for the headings that are displayed are selected; those that are hidden are not selected.

4. Select or deselect the headings as desired.

   The table changes to reflect your choice.

Filtering Users

You can filter users based on the contents of the columns on the User Accounts page.

To filter users:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **User Accounts**.

   The User Accounts page appears, displaying the users in tabular format.

2. Click the down arrow to the right of any column heading.

3. Select **Filters**.

   The filter field appears, with a **Go** button to the right of it.

4. Enter or select the filter criteria and click **Go**.

   On applying the filters, the table contents shrink to display the values that match the filter applied. The criteria by which the display is filtered and the column heading appear just above the table.

> **NOTE:** Filters applied across multiple columns have an additive effect; that is, each succeeding filter further restricts the display.

5. To remove a filter, click the [X] icon to the right of the filter criteria shown just above the table. For more information about filtering based on the contents of columns, see the "Inventory Landing Page Overview" on page 129 topic in the *Junos Space Network Management Platform User Interface Guide*.

Viewing User Details

You can view the details of users on the User Accounts inventory page.

To view detailed user information:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **User Accounts**.

   The User Accounts page appears, displaying the users configured in Junos Space Platform in tabular format.

2. Perform one of the following tasks:

   - Select a user and click the **Display Quick View** icon on the menu bar.

     The following information is displayed to the right of the selected user:

     - Login ID
     - First Name
     - Last Name
     - Email
     - User Type
     - Locked Out
     - Password Status

     For information about the fields, see Table 128.

     To hide the quick view, click the **Hide Quick View** icon on the menu bar.

   - Double-click a user row in the table.

     The User Detail Summary page appears, showing the information described in Table 128.

Table 128: User Detail Summary Page

Field Name	Description
Login ID	Login username. This could be an e-mail address, but it need not match the e-mail address that might be provided in the Email field for that username.
First Name	First name of the user
Last Name	Last name of the user
Email	(Optional) User's e-mail account. The e-mail address provided here need not match the login ID, if the login ID is also an e-mail address.
User Type	Whether the user is created manually (**Local**) or automatically by Junos Space Network Management Platform through remote login (**Remote**) For more information about local and remote users, see the flowcharts in "Configuring a RADIUS Server for Authentication and Authorization" on page 1473.
Status	Whether the user is **Enabled** or **Disabled**. Users are enabled by default. Disabling a user is not the same as deleting a user. A user whose account is disabled cannot log in to the Junos Space server.
GUI Access	Whether the user has GUI access
API Access	Whether the user has API access
Use global settings	Whether the global settings must be used to determine the maximum number of concurrent UI sessions permitted for the user
Maximum concurrent UI sessions	Maximum number of concurrent UI sessions permitted for the user If this field is set, then this value overrides the global settings.
Locked Out Status	Whether a user is locked out A locked-out user cannot log in to the Junos Space server. Such users must request the administrator to unlock their user accounts.
Password Status	Whether a user's password is expired or active The term "Temporary" is displayed for temporary passwords.
View Jobs	Job-related permissions assigned to the user: View All Jobs or View User's Own Job Only

Table 128: User Detail Summary Page *(continued)*

Field Name	Description
Certificate	E-mail address, common name, organizational unit, organization, location, state, and country of the certificate user The View Certificate Detail link displays more details about the certificate.
X.509 Certificate Parameters	X.509 certificate parameter values of the user This field is displayed only if the parameters are defined and the certificate parameter–based or password-based mode is enabled.
Assigned Roles	Predefined user roles assigned to the user
Assigned Domains	Domains to which the user is assigned Users can access only those objects within the domain to which they are assigned. By default, all users are assigned to the global domain, if the users are not assigned to a specific domain.
Role Summary	Name of the applications to which the roles belongs, and list of permissions attached to the roles

3. • To view the details of the certificate, click the **View Certificate Detail** link.

   The X.509 Certificate Detail dialog box is displayed. Table 129 displays the fields in the dialog box.

   Table 129: X.509 Certificate Detail Page

Field	Description
Subject Name	E-mail address, common name, organizational unit, organization, location, state, and country of the certificate user
Issuer Name	E-mail address, common name, organizational unit, organization, location, state, and country of the certificate issuer
Signature Algorithm Name	Algorithm used by the certificate authority or issuer to sign the certificate.
Serial Number	Serial number of the certificate
Not Before	Date at which the certificate became valid
Not After	Date at which the certificate will become invalid

   • Click **Close** to close the X.509 Certificate Detail dialog box.

4. To close the User Detail Summary page, click **OK** at the bottom of this page or the [X] icon in the upper-right corner of this page.

Performing Actions on Users

You can perform the following actions from the Users Accounts page:

- **Modify User**—See "Modifying a User" on page 1044.
- **Delete Users**—See "Deleting Users" on page 1050.
- **Clear Local Passwords**—See "Clearing User Local Passwords" on page 1067.
- **Disable Users** and **Enable Users**—See "Disabling and Enabling Users" on page 1051.
- **Unlock Users**—See "Unlocking Users" on page 1053.
- **Delete Private Tags**—Delete tags that you created.
- **Tag It**—See "Tagging an Object" on page 1526.
- **UnTag It**—See "Untagging Objects" on page 1527.

- **View Tags**—See "Viewing Tags for a Managed Object" on page 1532.
- **Clear All Selections**—All selected users on the User Accounts inventory page are deselected.

RELATED DOCUMENTATION

Configuring Users to Manage Objects in Junos Space Overview | **1033**

Creating Users in Junos Space Network Management Platform | **1035**

Deleting Users | **1050**

Modifying a User | **1044**

Viewing User Statistics | **1068**

Tagging an Object | **1526**

Viewing Tags for a Managed Object | **1532**

Exporting User Accounts from Junos Space Network Management Platform

IN THIS SECTION

Creating a User Accounts Report Definition | **1062**

Generating and Downloading a Report | **1063**

You can export user accounts from the Junos Space Network Management Platform database and download them to your local computer in CSV, PDF, and HTML formats.

Perform the following tasks to export user accounts from Junos Space Platform:

Creating a User Accounts Report Definition

You need to create a User Accounts report definition, using which you can create and export a user account report.

To create a User Accounts report definition on Junos Space Platform:

1. On the Junos Space Platform user interface, select **Reports** > **Report Definitions**.

   The Report Definitions page that appears displays all the report definitions that currently exist in the Junos Space Platform database.

2. Click the **Create Report Definition** icon on the toolbar.

   The Create Report Definition page is displayed.

3. In the **Report Name** field, type a report definition name.

   A report definition name cannot exceed 128 characters and can contain only letters, numbers, spaces, and the following special characters: hyphen (-), underscore (_), period (.), at (@), single quotation mark (’), forward slash (/), and ampersand (&).

4. (Optional) In the **Description** field, type a description.

   The description cannot exceed 512 characters.

5. Click the Add icon below the Description field to select the attributes of the report definition.

   The Select Report Type dialog box is displayed.

6. Select the check box next to the User Accounts report type.

7. Click **Add**.

   The User Accounts report type is added to this report definition.

8. (Optional) You can add filters to the report definition to customize the User Accounts report.

   To add a filter:

   a. Click the pencil icon in the Filter column.

      The Edit Columns/Filters dialog box is displayed. Add the filters using this dialog box. For more information about how to add filters, see “Creating Report Definitions” on page 780.

   b. Click **OK**.

The filters you selected are added to the report definition. The reports generated using this report definition display only those items that meet the filter criteria.

9. Click **Create**.

   The new report definition is created and you are redirected to the Report Definitions page.

Generating and Downloading a Report

You can generate and download reports by using the User Accounts report definition that you created.

To generate and download a report:

1. On the Junos Space Network Management Platform user interface, select **Reports** > **Report Definitions**.

   The Report Definitions page that appears displays all report definitions that currently exist in the Junos Space Platform database.

2. Right-click the User Accounts report definition that you created and select **Generate Report**.

   The Generate Reports dialog box is displayed.

3. (Optional) Next to the **Report Format** field, select the check boxes adjacent to the report formats that you want to generate.

   You can generate reports in CSV, HTML, and PDF formats. By default, all three check boxes are selected.

4. (Optional) Select the check box next to the SCP Server label to store the report in a directory on an SCP server.

   If you selected to store the report in a directory on the SCP server:

   a. In the **IP Address** field, enter the IP address of the SCP server.

      NOTE:
      - Depending on whether the Junos Space fabric is configured with only IPv4 addresses or both IPv4 and IPv6 addresses, Junos Space Platform allows you to enter an IPv4 address or either an IPv4 or IPv6 address respectively for the SCP server.
      - The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to http://www.iana.org/assignments/ipv4-address-space for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space for the list of restricted IPv6 addresses.

   b. From the **Port** spin box, select the appropriate port number.

By default, 22 is selected.

c. In the **Directory** field, enter the directory on the SCP server where the report must be stored.

d. In the **User Name** field, enter the username used to access the SCP server.

e. In the **Password** field, enter the password used to access the SCP server.

5. (Optional) Select the check box next to the Email label to add e-mail addresses of users who need to receive the report.

   If you selected to add the e-mail address of a user who needs to receive the report:

   a. In the **Email Address** field, enter the e-mail address of the user.

   b. Click **Add**.

      You can add multiple e-mail addresses if you want the report to be delivered to multiple users.

6. (Optional) Select the **Schedule at a later time** check box to schedule a date and time at which to generate the report automatically.

7. (Optional) Select the **Recurrence** check box and specify the frequency at which to generate the report.

8. Click **Generate**.

   The Generated Report Job Information dialog box that appears displays details about the generated report.

9. Click **OK**.

   You are redirected to the Reports page.

10. Select **Reports > Generated Reports** from the task tree.

    The Generated Reports page that appears displays a list of the generated reports.

11. Click the **View/Download** link corresponding to the report that you want to view or download.

    The View Report dialog box that appears displays the details of the report that you generated.

12. Click the button corresponding to the format of the report that you want to view or download to your local computer.

    You can view and download reports in CSV, PDF, and HTML formats.

13. Save the report to your local computer.

Click **Close** to return to the Generated Reports page.

RELATED DOCUMENTATION

Reports Overview | 768

Creating Report Definitions | 780

Creating Users in Junos Space Network Management Platform | 1035

Changing Your Password on Junos Space

After you log in to Junos Space Network Management Platform, you can change your password using the User Settings icon on the Junos Space banner. You do not require any particular Junos Space role to change your password. After a password change, you are logged out of the application. You must login again with the new password. If you use REST API to change the password, you must use Basic Auth to change the password, instead of using session ID or cookies.

Starting with Junos Space Platform Release 12.1, Junos Space has implemented a default standard for passwords that is compliant with the industry standard for security.

NOTE:

- When you upgrade to Junos Space Platform Release 12.1 or later, the default standard takes effect immediately. All local users receive password expiration messages the first time they log in to Junos Space after the update.
- You need to have set your local password to be able to change it. If you do not have a local password set, you will not be able to set or change it.
- You can use the **User Settings** icon to change only your local password. The change does not affect any passwords that an administrator might have configured for you on a remote authentication server.

To change your local password:

1. On the Junos Space Platform UI, click the **User Settings** icon on the right side of the Junos Space banner.

   The **Change User Settings** dialog box appears.

2. In the **Old Password** text box, enter your old password.

> **NOTE:** Mouse over the information icon (small blue *i*) next to the **New Password** text box to view the rules for password creation. For more information about the password rules, see "Modifying Junos Space Network Management Platform Settings" on page 1346.

3. In the **New Password** text box, enter your new password.

4. In the **Confirm Password** text box, enter your new password again to confirm it.

> **NOTE:** The fields on the **X.509 Certificate** tab are applicable when you want to use certificate-based authentication. If you are using password-based authentication, you can ignore these fields. For more information about certificate-based authentication, see the "Certificate Management Overview" on page 1426 topic in the *Junos Space Network Management Platform Workspaces Feature Guide*.

5. (Optional) Select the **Manage objects from all assigned domains** check box on the **Object Visibility** tab to view and manage objects from all the domains that you are assigned to.

6. Click **OK**.

   You are logged out of the system. To log in to Junos Space again, you must use your new password. Other sessions logged in with the same username are unaffected until the next login.

RELATED DOCUMENTATION

Logging In to Junos Space | 100

Junos Space User Interface Overview | 89

Clearing User Local Passwords

Junos Space Network Management Platform allows for an emergency password (authentication server down) to be set if in remote authentication mode, or allows the user to be handled locally (remote authentication fails) if in remote-local authentication mode. You can remove the local password you assign to users with remote or remote-local authentication by using the Clear Local Passwords action.

To remove one or more user local passwords, you must have User Administrator privileges.

To remove a user local password:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **User Accounts**.

   The User Accounts inventory page appears.

2. Select one or more users for which you want to remove a local password.

3. Select **Clear Local Passwords** from the Actions menu.

   This option is disabled (dimmed) if you try to clear the password for a local user. When you mouse over the option, the following tooltip is displayed:
   The following users are local only, so their passwords cannot be cleared: user1

   The **Clear Local Passwords** dialog box appears.

4. Click **Clear Passwords**.

   The local passwords of the selected user accounts are cleared.

RELATED DOCUMENTATION

Viewing Users | **1054**

Creating Users in Junos Space Network Management Platform | **1035**

Modifying a User | **1044**

Creating a Remote Authentication Server | **1468**

Viewing User Statistics

You can view the percentage and the number of Junos Space Network Management Platform users that have been assigned to a role.

- Viewing the Number of Users Assigned by Role | **1068**

Viewing the Number of Users Assigned by Role

To view the percentage of total users that have been assigned to a role:

1. On the Junos Space Network Management Platform user interface, click **Role Based Access Control**.

   The Role Based Access Control statistics page appears.

   Junos Space Network Management Platform displays a bar chart showing users by assigned role.

   The bar chart displays the number of users assigned to each role that has one or more assigned users.

   - To view the number of users assigned to a specific role, mouse over the role in the chart.
   - To display an inventory page of users assigned to a specific role, click the segment of the chart that represents the role.

RELATED DOCUMENTATION

Role-Based Access Control Overview | **995**

Viewing Users | **1054**

Creating Users in Junos Space Network Management Platform | **1035**

Deleting Users | **1050**

CHAPTER 61

User Groups

IN THIS CHAPTER

- User Groups Overview | 1069
- Managing User Groups | 1070
- Job Management Using User Groups | 1074

User Groups Overview

A user group is a collection of users who can view the jobs of all the users assigned to the user group.

Junos Space Management Platform provides an enhanced workflow to manage logical groups or user groups. In this workflow, you can perform the following operations with user groups:

- Create a user group and assign user(s) to it.
- Modify an existing user group by assigning more users to it, or removing existing users using the Assign or Unassign options respectively.
- Delete user groups if they are not required anymore.
- Search for a particular user in a user group.
- Filter users in a user groups as required.
- View details of a user group.

Once the user(s) are added to a group, then by default, user can view his own jobs and assigned group members job regardless of the user's job visibility permission.

NOTE:

- Only a Junos Space Super Administrator, User Administrator, or a user assigned to a custom role that provides permissions to manage user groups can create and manage user groups.
- A Super Administrator cannot be assigned to any user groups.

RELATED DOCUMENTATION

Managing User Groups | 1070
Job Management Using User Groups | 1074

Managing User Groups

The following sections discuss the operations a Super Administrator or a User Administrator can perform with user groups.

Creating a User Group

To create a user group:

1. On the Junos Space Management Platform UI, select **Role Based Access Control** > **User Groups**.

   The User Groups page appears.

2. Click **(+)** icon on the toolbar or right-click on **Groups** and select **Create User Group**.

   The User Group Information page appears. This page displays the User Group Information area on the left of the page and the Create User Group area on the right of the page.

3. In the Group Name field, enter the name of the user group.

   The group name cannot exceed 50 characters and cannot contain commas, double quotation marks, or parentheses, and cannot start with a space.

4. (Optional) In the Description field, add a description for the user group.

5. Click **Next** at the lower-right corner of the page.

   The Assign User for <*Group Name*> page appears. You can assign users to the user group from this page. All users (including remote users) except the super user are listed in a table and available for selection.

6. You can select users from the table, search for users by using keywords, and filter users by using tags or columns.

   - To select users by using keywords, enter the keyword in the Search field and click the Search icon. The list of users in the table is filtered by the keyword.
   - To filter users by their properties, select the check box next to the appropriate column on the Column Filter drop-down list.

- To filter users by tags, select an appropriate tag from the Tag Filter drop-down list.
- To select all users, select the **Select all items across all pages** check box.
- To select some users from the table, select the check box next to their usernames.
- To reset all filters, click **Reset All**.

> **NOTE:** You can add a maximum of 100 users to a user group.

7. After selecting all the users that you want to assign to the user group, click **Finish** on the lower-right corner of the page.

   The new user group is created. The User Groups landing page appears and the new user group is listed under **Groups**.

8. Click on the user group name to view the details of the user group on the right-side pane.

   The details of the user group such as the Group Name, Description, Date and Time Created, Assigned Users (number), and the users assigned to the user group is displayed on the pane. You can review the user group information.

   You can also search for users present in the user group based on keywords, tags, or columns.

   The Assigned Groups column displays the user groups to which each user is assigned to. If a user is assigned to more than one user group, a hyper-link **Multiple Groups** appears in the Assigned Groups column for that user. Click **Multiple Groups** and **Groups assigned to the User** page appears. This page lists the user groups to which the user is assigned.

9. You can also assign or remove users from the user group from this pane. To assign a user to the user group, click on the Assign **(+)** icon available on the top-left corner of the table.

   The Assign Users to Group page appears. Select the users you want to add the user group (you can follow the procedure described in step 6 to select the users) and click **Assign**.

   The selected users are assigned to the user group.

10. If you want to remove users from the user group, select the users in the table and click the **(-)** icon available on the top-left corner of the table.

    The selected users are removed from the user group.

NOTE: When a user is assigned to a user group, or is a user is removed from a user group, the user's session is automatically terminated. The user will have to re-log in to Junos Space Management Platform for the user group assignment to take effect for the user.

Modifying a User Group

To modify a user group:

1. On the Junos Space Platform UI, select **Role Based Access Control** > **User Groups**.

   The User Groups page appears. The existing user groups are listed under Groups.

2. To modify the user group name and description, right-click on the user group and select **Modify User Group**.

   The Modify User Group page appears. Update the user group name and description as required and click **Save**.

3. To assign a user to a user group, click on the user group name.

   The details of the user group appears on the right-side pane.

4. Click the Assign **(+)** icon available on the top-left corner of the table.

   The Assign Users to Group page appears. Select the users you want to add the user group and click **Assign**.

   You can select users from the table, search for users by using keywords, and filter users by using tags or columns.

   - To select users by using keywords, enter the keyword in the Search field and click the Search icon. The list of users in the table is filtered by the keyword.
   - To filter users by their properties, select the check box next to the appropriate column on the Column Filter drop-down list.
   - To filter users by tags, select an appropriate tag from the Tag Filter drop-down list.
   - To select all users, select the **Select all items across all pages** check box.
   - To select some users from the table, select the check box next to their usernames.
   - To reset all filters, click **Reset All**.

The selected users are added to the user group.

5. If you want to remove users from the user group, select the users in the table and click the **(-)** icon available on the top-left corner of the table.

   The selected users are removed from the user group.

> **NOTE:** When a user is assigned to a user group, or is a user is removed from a user group, the user's session is automatically terminated. The user will have to re-log in to Junos Space Management Platform for the user group assignment to take effect for the user.

Deleting a User Group

To delete a user group:

1. On the Junos Space Platform UI, select **Role Based Access Control** > **User Groups**.

   The User Groups page appears. The existing user groups are listed under Groups.

2. To delete the user group, right-click on the user group and select **Delete User Group**.

   A confirmation message appears asking whether you want to delete the user group.

3. Click **Yes** if you want to delete the user group. Click **No** if you do not want to continue with this operation.

4. If you click **Yes**, the user group is deleted and you will see a success message that the user group is deleted.

> **NOTE:** When a user group is deleted, all the associated user's session is automatically terminated. The user will have to re-log in to Junos Space Management Platform for the user group assignment to take effect for the user.

RELATED DOCUMENTATION

User Groups Overview | **1069**

Job Management Using User Groups | **1074**

Job Management Using User Groups

IN THIS SECTION

- Job Visibility for User Assigned to User Group(s) | 1074

A job is an action that is performed on any object that is managed by Junos Space, such as a device, service, or user. The Jobs workspace lets you monitor the status of jobs that have run or are scheduled to run, in Junos Space Network Management Platform and all installed Junos Space applications. Jobs can be scheduled to run immediately or in the future.

By default, when you log in as a non-administrator, you can view only your own jobs, which include jobs triggered by you as well as jobs reassigned to you. However, at the time of creation or modification of a user account or remote profile, a User Administrator, can explicitly configure the user account or remote profile to view all jobs triggered by all users across all applications.

> **NOTE:** By default, a user with the Super Administrator or Job Administrator role can view all jobs triggered by all users across all applications.

Junos Space Network Management Platform supports job visibility in the following two ways:

- View User's Own Jobs Only—Enables the users to view the jobs created by them or assigned to them.
- View All Jobs—Enables the user to view all the jobs.

For more information on jobs and job management, see "Jobs Overview" on page 965.

The following section discusses various cases of job visibility for users assigned to user groups.

Job Visibility for User Assigned to User Group(s)

Users assigned to a user group can view all the jobs created by, or assigned to all users in the user group. You can view the user groups to which a user is assigned in two ways:

- For Super Administrator or User Administrator—Go to **Role Based Access Control > User Groups** page and click on a user group name. The details of the user group appears on the right side of the page. In the table on the lower part of the page, the Assigned Groups column in page displays the user groups to which each user is assigned to. If a user is assigned to more than one user group, a hyper-link **Multiple Groups** appears in the Assigned Groups column for that user. Click **Multiple Groups** and **Groups assigned to the User** page appears. This page lists the user groups to which the user is assigned.

- For all users—Go to **Jobs > Job Management** page. The jobs associated to the user appears on the page. In the table, the Groups column in page displays the user groups to which each user is assigned to. If a user is assigned to more than one user group, the user groups are displayed as a comma separated list.

For example, user group Sample contains two users—user A and user B. In this case, both user A can view the jobs created or assigned to user A and user B. Similarly, User B will also be able to view jobs associated with user A and user B. Consider that user A has View All Jobs permission and user B has View User's Own Jobs Only permission.

When user A and user B are assigned to user group Sample, job visibility behavior is as follows:

> **NOTE:** By default, both user A and user B will be able to view all the jobs associated with user group Sample, regardless of their job visibility permissions.

- **Job Visibility for user A (View All Jobs permission)**—User A can view only the jobs associated with the user group Sample, despite having View All Jobs permission. That is, being assigned to a user group restricts user A's job visibility to only view the jobs associated with the user group.

  If user A wants to view all the jobs (not just jobs associated with user group Sample), user A must perform the following steps:

  1. On the Junos Space Platform UI, click the User Settings icon on the right side of the Junos Space banner.

     The Change User Settings dialog box appears.

  2. Select the **Group Visibility** tab.

     The Group Visibility tab appears. By default, the Enable Group Visibility check box is selected.

  3. Clear **Enable Group Visibility** check box and click **OK**.

  User A will now be able to view all the jobs created in the system.

- **Job Visibility for user B (View User's Own Jobs Only permission)**—User B can view all the jobs associated with the user group Sample, despite having View User's Own Jobs Only permission. That is, even though user B's job visibility permission only allows him to view only his jobs, being assigned to a user group allows user B to view all the jobs associated with the user group.

  If user B wants to view only his own jobs (not jobs associated with user group Sample), user B must perform the following steps:

  1. On the Junos Space Platform UI, click the User Settings icon on the right side of the Junos Space banner.

     The Change User Settings dialog box appears.

  2. Select the **Group Visibility** tab.

The Group Visibility tab appears. By default, the Enable Group Visibility check box is selected.

3. Clear **Enable Group Visibility** check box and click **OK**.

User B will now be able to view only his own jobs.

RELATED DOCUMENTATION

- User Groups Overview | **1069**
- Managing User Groups | **1070**
- Jobs Overview | **965**

CHAPTER 62

Domains

IN THIS CHAPTER

- Domains Overview | 1077
- Working with Domains | 1085
- Assigning Objects to an Existing Domain | 1092
- Exporting Domains from Junos Space Network Management Platform | 1096

Domains Overview

IN THIS SECTION

- Accessing Objects In and Across Domains | 1078
- Device Partitions | 1080
- Assignment of Objects to Domains | 1083

In Junos Space Network Management Platform, a domain is a logical mapping of objects, such as devices, device templates, and CLI Configlets, to users who access and manage the network by using these objects. Junos Space Platform allows a hierarchal structure for domains. The top-level domain is called the Global domain. You can create a hierarchy of up to five levels of subdomains under the Global domain, with each subdomain associated with only one parent domain. You can use these subdomains to create easily manageable sections of your network. When you assign objects and users to these subdomains, users can manage these objects partially or completely based on the roles assigned to them. Objects created in a domain are assigned to the same domain.

Using Junos Space Platform, you can create objects with the same name across domains; however, domains at the same hierarchy level cannot share the same name. The domain association is displayed in fully qualified domain name (FQDN) format in the Domain column of all workspaces.

You can create the following objects with the same name across domains:

- Templates and template definitions
- CLI Configlets, configuration views, XPath, regular expressions, and configuration filters
- Report definitions
- Images, script bundles, and operations

Users can be assigned to multiple domains. Objects are assigned to the domain to which the user is logged in currently. Junos Space Platform lets you assign multiple objects from the same workspace to a domain simultaneously. The domain to which an object is assigned is displayed in the Domain column on the inventory page of the workspace. This is displayed as an absolute path.

The default Super Administrator “super”’ has full permissions to all subdomains. You need not manually assign new subdomains to this Super Administrator. You need to assign the Global domain to all users who are added to the Junos Space Platform database with the Super Administrator role.

You cannot delete the Global domain from Junos Space Platform. Junos Space Platform also does not allow you to delete a domain if subdomains are associated with that domain.

You can view predefined objects in a Junos Space Platform or Junos Space application workspace in addition to the objects that are assigned to the domain in which you are currently operating. To access workspaces on a Junos Space application that is installed on Junos Space Platform, the workspaces must be domain aware. Only domain-aware workspaces of an application can be accessed from the subdomains. When you switch between domains, you could lose access to workspaces if the application is not domain aware.

> **NOTE:** If you access the Junos Space Platform UI in two tabs of the same browser with two different domains selected and access the same page in both tabs, the information displayed on the page is based on the latest domain selected. To view pages that are accessible only in the Global domain, ensure that you are in the Global domain in the most recent tab in which you are accessing the UI.

The following sections explain the rules to access objects across domains and how device partitions are used to manage subdomains:

Accessing Objects In and Across Domains

Junos Space Platform allows you to access objects across domains based on the roles you are assigned and the domains you are assigned to.

The following rules apply while accessing objects across domains in Junos Space Platform:

- Objects can be assigned to only one domain.
- Objects can be moved from one domain to another.

- Objects across domains can share the same name.
- You can view objects from the parent domain only in read-only mode and only if the parent domain allows its objects to be viewed by its subdomains.
- You can view and execute tasks on objects in a subdomain if the object is provided with appropriate permissions.
- You cannot modify or delete objects in a parent domain if you have read-only access, even if you have the necessary permissions to modify those objects.
- You can view and perform actions only on the objects assigned to the domain to which you are currently logged in. You can view objects from other accessible domains if the "Manage objects from all assigned domains" flag is set as a user preference. To set this flag, click the User Settings icon on the Junos Space banner.
- If you have read/write privileges to objects in a subdomain, you can perform read/write operations on the objects in the subdomain even if the subdomain is not explicitly assigned to you.
- If you have read-only privileges to objects in a subdomain, you can perform only read operations on the objects in the subdomain.
- If you have read-only access to objects in the parent domain, you cannot perform write operations even if you have read/write privileges on these objects by virtue of the roles assigned to you.
- If you do not have read-only access to objects in the parent domain, the objects in the parent domain are not visible to you in the subdomain.

In addition to the default rules to access objects assigned to domains, you can also use the “Allow users of this domain to have read and execute access to parent domain objects” flag to provide read permissions to all users in the domain when you create a domain. This flag provides both read and execute access to the objects in the parent domain.

If you use this flag, you can access the following objects that have read and execute permissions:

- Device templates and template definitions
- CLI Configlets, configuration views, configuration filters, XPath, and regular expressions
- Images, scripts, operations, and script bundles
- Report definitions

Device Partitions

Use device partitions to share physical interfaces, logical interfaces, and physical inventory of devices among multiple subdomains. Device partitions are supported only on M Series and MX Series routers.

Consider the following restrictions when working with device partitions:

- You can assign only one partition of a device to a subdomain; you cannot assign multiple partitions of the same device to a subdomain.
- You can assign one partition each from multiple devices to a subdomain.
- You can partition a device only if the device is currently assigned to the Global domain.
- To assign a partition to a subdomain, the root device should be part of the Global domain.

For example, consider device D1 with partitions P1, P2, and P3; device D2 with partitions P1a and P2a; and Global, dom1, and dom2 to be the available domains in Junos Space. The following assignments of partitions are valid:

- P1 to dom1
- P1a to dom1
- P2 to dom2
- P2a to dom2
- P3 to Global (default)

The following assignments are invalid: P1 and P2 to dom1 or P1a and P2a to dom2.

To assign a partition to a subdomain, the root device must be part of the Global domain.

Table 130 lists the actions that you can or cannot perform on a device partition:

Table 130: Tasks Supported on Device Partitions

Task Group	Task Name	Device Partition Support	Notes
Device Configuration	Review/Deploy Configuration	No	–
	View/Edit Configuration	No	–
	View Active Configuration	Yes	Configuration details are not filtered on the basis of the partitioning.
	Resolve Out-of-band Changes	No	–
	View/Assign Shared Objects	No	–
	View Configuration Change Log	Yes	Configuration details are not filtered on the basis of the partitioning.
	View Template Deployment	No	–
	View/Edit Unmanaged Device Configuration	No	–
Device Inventory	Export Physical Inventory	No	–
	View Associated Scripts	Yes	–
	View License Inventory	No	–
	View Logical Interfaces	Yes	–
	View Physical Interfaces	Yes	–
	View Physical Inventories	Yes	–
	View Script Execution	Yes	–
	View Inventory Change	Yes	–
	View Software Inventory	No	–
Device Operations	Create LSYS	No	LSYS should be managed only on the root device.

Table 130: Tasks Supported on Device Partitions *(continued)*

Task Group	Task Name	Device Partition Support	Notes
	Delete Devices	No	You cannot delete a device partition from the subdomain.
	Looking Glass	No	–
	Put in RMA State	No	This action can be performed only on the root device.
	Reactivate from RMA	No	This action can be performed only on the root device.
	Synchronize with Network	No	This action can be performed only on the root device.
	Execute Script	Yes	–
	Apply CLI Configlet	Yes	–
Device Access	Modify Authentication	No	This action can be performed only on the root device.
	Launch Device WebUI	No	This action can be performed only on the root device.
	SSH to Device	No	This action can be performed only on the root device.
	Resolve Key Conflict	No	This action can be performed only on the root device.
Managed Customized Attribute		No	–
Delete Private Tags		No	–
Tag It		No	–

Table 130: Tasks Supported on Device Partitions *(continued)*

Task Group	Task Name	Device Partition Support	Notes
Un Tag It		No	–
View Tags		No	–
Filter by CSV		Yes	–
Clear All Selection		Yes	–

You can assign device partitions to a domain or move the device partition from one domain to another. To assign a device partition to a domain or move a device partition from one domain to another, right-click the device partition and select **Assign Partition to Domain**.

You can assign devices to a domain. To do so, right-click the device and select the **Assign Device to Domain** task. You cannot move devices with partitions to a subdomain. If you do so, the **Assign Device to Domain** job fails.

Assignment of Objects to Domains

Objects in Junos Space Platform workspaces are assigned to at least one of the available domains.

The following rules apply while managing objects in the various workspaces:

- Templates—Templates and template definitions are created in the domain that you are currently operating in. When you create a template, you can select a template definition from the same domain or a parent domain if you have access to the parent domain. You can deploy templates on devices if they are in the same domain or if devices belong to other accessible domains and the “Manage objects from all assigned domains” flag is set as a user preference. To set this flag, click the User Settings icon on the Junos Space banner. Also, you can deploy templates that are inherited from the parent domain to the devices in the accessible domains.
- CLI Configlets—CLI Configlets are assigned to the domain that you are currently operating in. You can apply CLI Configlets to devices if they belong to the same domain or if the devices belong to other accessible domains and the “Manage objects from all assigned domains” flag is set as a user preference. You can assign and deploy CLI Configlets that are inherited from the parent domain to the devices in the current domain.
- Images and Scripts—Images and scripts are assigned to the domain that you are currently operating in. You can stage, deploy, or perform any action on images and scripts for only those devices that belong to the same domain or if the devices belong to other accessible domains and the “Manage objects from

all assigned domains" flag is set as a user preference. You can also inherit images and scripts from the parent domain and perform some actions such as staging on devices in the current domain and other accessible domains.

- Configuration Files—Configuration files are created in the domain to which the device is currently assigned. If a device is moved from one domain to another, configuration files are also automatically moved to the respective domain. This workspace does not display objects inherited from the parent domain if the "Manage objects from all assigned domains" flag is set as a user preference.
- Jobs—Jobs are associated with the domain from which you initiate jobs. You can view jobs from other domains that are assigned to you if the "Manage objects from all assigned domains" flag is set as a user preference.
- Audit Logs—Audit logs are generated in the domain from which the user initiated the actions. You can view audit logs from other domains that are assigned to you if the "Manage objects from all assigned domains" flag is set as a user preference.
- Role Based Access Control—The Roles page is not available in the subdomains. You can create users only when you are logged in to the Global domain. You can assign users to a domain when or after you create user accounts.
- Administration—You can access the complete Administration workspace only if you are logged in to the Global domain.
- Reports—Report definitions are assigned to the domain in which they are created. You can generate reports by using the definition in the inherited domain or the current domain.

NOTE: Global search displays objects that match the search query from the current domain, child domains, and parent domain (if the user has read-only access to the parent domain). If an object in the search results is in a different domain than the one the user is currently in, the hyperlink to the object in the search results is disabled.

RELATED DOCUMENTATION

Working with Domains | **1085**

Exporting Domains from Junos Space Network Management Platform | **1096**

Working with Domains

IN THIS SECTION

- Adding a Domain | 1085
- Modifying a Domain | 1087
- Deleting Domains | 1089
- Switching from One Domain to Another | 1092

You add a domain to Junos Space Network Management Platform to assign users, devices, and other objects to that domain. You can add, modify, and delete a domain from the Role Based Access Control workspace only if you have the privileges of a Domain Administrator and are logged in to the Global domain. You cannot create domains if you are logged in or have switched to any other domain.

Adding a Domain

You add a domain when you want to create a logical grouping of objects and users. You add a domain from the Role Based Access Control workspace. Junos Space Platform allows you to add up to five levels of subdomains under the Global domain. When you add a domain, a subdomain is created under the domain that you select.

To add a domain:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **Domains**.

   The Domains page is displayed.

   The Domains area on the left of the page displays the domains that are currently available in tree view. The right of the page displays the details of the domain that is currently selected in the Domains area. By default, the **Global** domain is selected.

2. In the Domains area, right-click the parent domain under which you want to create a domain and select **Create Domain**.

   This page displays two areas: Domain Information on the left and Create Domain on the right. The Create Domain area displays steps to create a domain.

3. In the **Domain Name** field, enter the name of the domain.

The domain name cannot exceed 255 characters and cannot contain commas, double quotation marks, or parentheses. Also, the name cannot start with a space.

4. (Optional) Select the **Allow users of this domain to have read and execute access to parent domain** check box if you want to allow users of this domain to have read and execute access to the objects in the parent domain.

5. (Optional) In the **Description** field, add a description of the domain.

6. Click **Next** in the lower-left corner.

   The Assign Users for Domain page is displayed. You can assign users to the domain from this page. All users except the super user are listed in a table and available for selection.

7. You can select users from the table, search for users by using keywords, and filter users by using tags or columns.

   - To select users by using keywords, enter the keyword in the Search field and click the Search icon.

     The list of users in the table is filtered by the keyword.

   - To filter users by their properties, select the check box next to the appropriate column on the **Column Filter** drop-down list.
   - To filter users by tags, select an appropriate tag from the **Tag Filter** drop-down list.
   - To select all users, select the **Select all items across all pages** check box.
   - To select some users from the table, select the check box next to their usernames.
   - To reset all filters, click **Reset All**.

   > **NOTE:** Filtering columns such as Assigned Domains can help you assign users across domains quickly and effectively.

8. Click **Next**.

   The Assign Devices for Domain page is displayed. You can assign devices to the domain from this page. All devices that are discovered to Junos Space Platform are listed in a table on this page.

9. You can select devices from the table, search for devices by using keywords, and filter devices by using tags or columns.

- To select devices by using keywords, enter the keyword in the Search field and click the Search icon.

  The list of devices in the table is filtered by keyword.
- To filter devices by their properties, on the **Column Filter** drop-down list, select the check box next to the appropriate column and enter the keyword in the Search field.
- To filter devices by tags, select an appropriate tag from the **Tag Filter** drop-down list.
- To select all devices, select the **Select all items across all pages** check box.
- To select some devices from the table, select the check boxes next to their names.

> **NOTE:** To reset all filters, click **Reset All**.

10. Click **Finish**.

    A message box displays the job ID.

- You can click the job ID to see the details of the job.

  You are redirected to the Job Management page with a filtered view of the job corresponding to the addition of domain. Click the job to view the Assign Device(s) to Domain Report with details of the status of the job.

- Click **OK**.

  You are redirected to the Domains page.

> **NOTE:** When the new domain is created, an informational message about switching domains is displayed in a dialog box.
>
> Do one of the following:
>
> - To prevent the informational message from appearing again, ensure that the **Don't show again** check box is selected and click **OK**. The **Don't show again** check box is selected by default.
> - To allow the informational message to continue appearing, clear the **Don't show again** check box and click **OK**.

Modifying a Domain

Only a user with the Domain Administrator role can modify a domain.

To modify a domain:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **Domains**.

   The Domains page appears.

2. Select the domain that you want to modify from the left pane.

   The right pane displays details about the selected domain.

3. Click the **Modify** icon on the left pane.

   The Modify Domain dialog box appears.

4. Make the necessary changes to the domain by using the Modify Domain dialog box.

   You can modify the domain name and description and allow or prevent users to have or from having read-only access to objects in the parent domain.

5. Click **Save** to close the Modify Domain dialog box.

6. On the right pane, assign or unassign users as required.

   To assign users to this domain:

   a. Click the (**+**) icon (**Assign Users**) on the right pane.

      The Assign Users page appears, displaying the Junos Space users except the super user and users who are already associated with this domain.

   b. Select one or more users to assign to this domain

      You may want to sort the data in any of the columns on the Assign Users page to quickly identify the users.

   c. Click **Assign**.

      You are returned to the Domains page, which displays the users that you added to this domain.

   To unassign users from this domain:

   a. Select users whom you no longer want to associate with this domain.

   b. Click the (**–**) icon (**Unassign Users**) on the right pane.

      The selected users are unassigned from this domain.

> **NOTE:** If one of the selected users belong only to this domain and not to any other domain, the delete action fails and the following error message is displayed:
> **User needs to be assigned to atleast one domain**

7. Click the **Assigned Devices** tab to assign devices to this domain. Use the (**+**) icon to achieve this task.

8. Click the **Assigned Remote Profiles** tab to add or remove remote profiles to or from this domain.
   a. Click the (**+**) icon (**Assign Remote Profiles**) on the right pane to add remote profiles.
   b. Click the (**-**) icon (**Unassign Remote Profiles**) on the right pane to remove remote profiles.

When you modify a domain, an audit log entry is generated.

Deleting Domains

Only a user with the Domain Administrator role can delete a domain.

Before you delete a domain, take the following points into consideration:

- All users who are logged in to the domain must be logged out.
- The domain is locked and users cannot move or log in to that domain unless the job fails.
- No objects must belong to the domain that is being deleted. You need to purge and archive audit logs and job data as well as move or delete devices and all other objects in that domain to another domain before you proceed with the deletion. You must trigger the deletion of a domain only after you ensure that there are no objects in that domain. If objects exist in the domain, the deletion job fails and a list of objects to be deleted is provided in the job description.
- Another administrator cannot create a domain with the same name as the domain that is being deleted until the domain deletion job is complete.
- You cannot delete the Global domain.
- You cannot delete a domain if the domain contains subdomains.

To delete a domain:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **Domains**.

   The Domains page appears.

2. Select the domain that you want to delete from the left pane.

3. Click the **Delete** icon on the left pane.

   A confirmation dialog box appears.

4. Click **Yes** on the confirmation dialog box to delete the domain.

   An information dialog box appears, displaying the job ID of the deletion job. Click the job ID to see whether the deletion of the domain is successful. If the job failed, then double-click the deletion job to determine the reasons for failure.

When the deletion of a domain fails, use the reasons listed in the job description of the domain deletion job to resolve the issue. Refer to the following example to view the reasons for the failure of a domain deletion job.

To view the reasons for the failure of a domain deletion job:

1. On the Junos Space Network Management Platform user interface, select **Jobs** > **Job Management**.

   The Job Management page appears.

2. Double-click the domain deletion job whose details you want to view.

   The Delete Domain Detail Report page appears. On this page, you see something similar to the following text in the Description column:

   a. **Delete or reassign following users before deleting domain: {test-user-1, test-user-2, }**

   b. **3 Device Object object[s] present in domain. Please remove or assign to another domain before deleting.**

   c. **162 Physical Interface Object object[s] present in domain. Please remove or assign to another domain before deleting.**

   d. **80 Physical Inventory Object object[s] present in domain. Please remove or assign to another domain before deleting.**

   e. **24 Logical Interface Object object[s] present in domain. Please remove or assign to another domain before deleting.**

3. Analyze the report and resolve the issue. In this example, resolve point b in the previous step, which is likely to address points c, d, and e because points c, d, and e are related to the devices in point b.

   You may encounter this error if a device is assigned to the domain being deleted and you are trying to delete that domain. To resolve this error, identify the devices that are assigned to this domain from

the Domains workspace and reassign the devices to another domain. For example, assume that one of the devices assigned to the domain that you are trying to delete is DeviceA.

To reassign DeviceA to the Global domain:

a. On the Junos Space Network Management Platform user interface, select **Devices** > **Device Management**.

   The Device Management page appears.

b. Select DeviceA.

c. Click **Assign to Domain** from the Actions menu.

   The Assign to Domain page appears, displaying all domains on the Junos Space server.

d. Click **Global**.

e. Click **Assign**.

   The selected device is reassigned to the Global domain.

4. Resolve point a, which states:
   Delete or reassign following users before deleting domain: {test-user-1, test-user-2, }

   You may encounter this error if a user is attached to only a single domain and you are trying to delete that domain. Identify the users assigned to this domain from the Domains workspace and reassign the users to another domain. In this example, reassign test-user-1 to the Global domain.

   To reassign test-user-1 to the Global domain:

   a. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **User Accounts**.

      The User Accounts page appears.

   b. Select test-user-1.

   c. Click the **Modify User** icon.

      The Modify User page appears.

   d. Click **Domain Assignment** on the right pane of the Modify User page.

   e. Select the **Global** check box.

   f. Click **Finish**.

The selected user is reassigned to the Global domain.

Repeat this procedure for test-user-2.

5. Try deleting the domain now. You should be able to delete the domain because you have resolved the issues that were preventing you from deleting the domain.

When you delete a domain, an audit log entry is automatically generated.

> **NOTE:** If you cannot delete a domain because there are jobs and audit logs associated with that domain, switch to the domain that contains the audit logs and jobs and purge them.

Switching from One Domain to Another

If you are a user who has access to multiple domains, then you can navigate from one domain to another by using the Domain drop-down list displayed at the top center of the Junos Space user interface.

> **NOTE:** If you access the Junos Space Platform UI in two tabs of the same browser with two different domains selected and access the same page in both tabs, the information displayed on the page is based on the latest domain selected. To view pages that are accessible only in the Global domain, ensure that you are in the Global domain in the most recent tab in which you are accessing the UI.

RELATED DOCUMENTATION

Domains Overview | **1077**

Assigning Objects to an Existing Domain

IN THIS SECTION

- Assigning Users to an Existing Domain from the Domains Page | **1093**
- Assigning Devices to an Existing Domain from the Domains Page | **1094**

Assigning Remote Profiles to an Existing Domain from the Domains Page | 1095
Assigning Objects to an Existing Domain from the Inventory Landing Pages | 1095

You assign users, devices, and remote profiles to an existing domain from the Domains page.

To assign users, devices, or remote profiles to an existing domain, navigate to the Domains page in the Role Based Access Control workspace.

The Domains area on the left of the page displays the domains that are currently available. The right of the page displays the details of the domains that you selected in the Domains area. The summary view at the top-right of the Domains page displays details such as the name of the domain, the description of the domain, the date and time the domain was created, the number of users assigned to the domain, the number of devices assigned to the domain, and the number of remote profiles assigned to the domain.

By default, the Global domain is selected. Select the domain to which you want to assign objects and perform any of the following tasks:

Assigning Users to an Existing Domain from the Domains Page

You can assign users to an existing domain from the Assigned Users tab of the Domains page.

To assign users to an existing domain from the Domains page:

1. Click the **Assigned Users** tab.

   The users that are currently assigned to the selected domain are displayed in a table.

   You can use the search field and the column and tag filters to filter users in the table in **Assigned Users** tab. You can also click any column name to sort users based on the column value. The paging controls enable you to browse through the list of users, and you can specify the number of users to be displayed per page by using the Show box.

2. To assign users, click the **Assign Users** icon below the tab.

   The Assign Users dialog box is displayed.

3. Select users:

   - To select users by using keywords, enter the keyword in the Search field and click the Search icon.

     The list of users in the table is filtered by keyword.

   - To filter users by their properties, select the check box next to the appropriate column on the **Column Filter** list.

- To filter users by tags, select an appropriate tag from the **Tag Filter** list.
- To select all users, select the **Select all items across all pages** check box.
- To select specific users from the table, select the check box next to the usernames.

> **NOTE:** Filtering columns such as Assigned Domains can help you assign users across domains quickly and effectively.

4. Click **Assign**.

   The selected users are assigned to the domain.

Assigning Devices to an Existing Domain from the Domains Page

You can assign devices to an existing domain from the Assigned Devices tab of the Domains page.

To assign devices to an existing domain from the Domains page:

1. Click the **Assigned Devices** tab.

   The devices that are currently assigned to the selected domain are displayed in a table.

   You can use the search field and the column and tag filters to filter devices in the table in **Assigned Devices** tab. You can also click any column name to sort devices based on the column value. The paging controls enable you to browse through the list of devices, and you can specify the number of devices to be displayed per page by using the Show box.

2. To assign devices, click the plus icon below the tab.

   The Assign Devices dialog box is displayed.

3. Select devices:
   - To select devices by using keywords, enter the keyword in the Search field and click the Search icon.

     The list of devices in the table is filtered by keyword.
   - To filter devices by their properties, select the check box next to the appropriate column on the **Column Filter** list.
   - To filter devices by tags, select an appropriate tag from the **Tag Filter** list.
   - To select all devices, select the **Select all items across all pages** check box.
   - To select specific devices from the table, select the check box next to the names of the devices.
4. Click **Assign**.

The selected devices are assigned to the domain.

Assigning Remote Profiles to an Existing Domain from the Domains Page

You can assign remote profiles to an existing domain from the Assigned Remote Profiles tab of the Domains page.

To assign remote profiles to an existing domain from the Domains page:

1. Click the **Assigned Remote Profiles** tab.

   The remote profiles that are currently assigned to the selected domain are displayed in a table.

   You can use the search field and the column and tag filters to filter remote profiles in the table in **Assigned Remote Profiles** tab. You can also click any column name to sort remote profiles based on the column value. The paging controls enable you to browse through the list of remote profiles, and you can specify the number of remote profiles to be displayed per page by using the Show box.

2. To assign remote profiles, click the plus icon below the tab.

   The Assign Remote Profiles dialog box is displayed. You can view the list of remote profiles in a table.

3. Select the remote profiles to assign to the domain from the table.

4. Click **Assign**.

   The selected remote profiles are assigned to the domain.

Assigning Objects to an Existing Domain from the Inventory Landing Pages

You can assign objects such as devices, remote profiles, template definitions, templates, CLI Configlets, configuration views, XPaths, regular expressions, configuration filters, report definitions, images, scripts, operations, and script bundles to a domain from their respective inventory landing pages.

To assign objects to an existing domain from the inventory landing pages:

1. Go to the respective inventory landing page. For example, go to the **Device Templates > Templates** page.

   The Templates inventory landing page that appears displays all the templates.

2. Select the templates to assign to the domain and select **Assign Template to Domain** from the Actions menu.

   The Assign Template to Domain dialog box is displayed. The domain tree lists all domains available in Junos Space Platform.

3. Select the domain to which you want to assign templates from the domain tree.

4. Click **Assign**.

   The selected templates are assigned to the domain.

Release History Table

Release	Description
16.1R1	The summary view at the top-right of the Domains page displays details such as the name of the domain, the description of the domain, the date and time the domain was created, the number of users assigned to the domain, the number of devices assigned to the domain, and the number of remote profiles assigned to the domain.
16.1R1	You can use the search field and the column and tag filters to filter users in the table in **Assigned Users** tab.
16.1R1	You can use the search field and the column and tag filters to filter devices in the table in **Assigned Devices** tab.
16.1R1	You can use the search field and the column and tag filters to filter remote profiles in the table in **Assigned Remote Profiles** tab

RELATED DOCUMENTATION

Domains Overview | **1077**

Working with Domains | **1085**

Exporting Domains from Junos Space Network Management Platform

You can export domains from the Junos Space Network Management Platform database and dowload them to your local computer as a single TAR file. This TAR file contains CSV files with the details of the exported domains. The CSV files contain details of all subdomains of the domain that you selected to export.

NOTE: You cannot export multiple domains that are at the same hierarchy level simultaneously.

To export domains from Junos Space Platform:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > Domains**.

   The Domains page is displayed. You can view the domain hierarchy on the left pane of this page.

2. On the left pane, right-click the domain that you want to export and select **Export Domain**.

   The Export Domain Confirmation dialog box that appears prompts you to confirm your selection.

3. Click **Yes** and save the TAR file to your local computer.

   The Export Domain Job Information dialog box displays details of the export domain job.

   Close the dialog box to return to the Domains page.

RELATED DOCUMENTATION

Domains Overview | **1077**

Working with Domains | **1085**

CHAPTER 63

Remote Profiles

IN THIS CHAPTER

- Creating a Remote Profile | 1098
- Modifying a Remote Profile | 1100
- Deleting Remote Profiles | 1101

Creating a Remote Profile

Remote profiles are used to assign a specific set of roles to users when remote authentication and authorization are enabled in Junos Space Network Management Platform. A remote profile is a collection of roles defining the set of functions that a user is allowed to perform in Junos Space Network Management Platform.

To create a remote profile:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **Remote Profiles**.

   The Remote Profiles page is displayed.

2. Click the **Create Remote Profile** icon on the menu bar.

   The Create Remote Profile page appears, displaying the Role Assignment area.

3. In the **Name** field, enter a name for the remote profile.

   The remote profile name cannot exceed 32 characters. The profile name can contain letters and numbers and can include a hyphen (-), underscore (_), or period (.).

4. In the **Description** field, enter a description for the remote profile.

   The remote profile description cannot exceed 256 characters. The description can contain letters and numbers and can include a hyphen (-), underscore (_), period (.), or comma (,).

5. Select the **GUI Access** and **API Access** check boxes depending on the type of access you want to allow for the remote profile.

   By default, the remote profile is able to access both the GUI and API. You should select at least one access type to successfully create a remote profile.

6. In the **Job Management View** section, retain the selection of **View User's Own Jobs Only** to enable remote users associated with this remote profile to view only their own jobs on the Job Management page. This option is selected by default, which means that all users can view only their own jobs.

   To allow a remote user associated with this remote profile to view all jobs triggered by all Junos Space users, select **View All Jobs**. By default, a user with the Super Administrator or Job Administrator role can view jobs of all users. When you create or modify a user with the Super Administrator or Job Administrator role, the Job Management View section is disabled and you cannot prevent such users from viewing all jobs.

   > **NOTE:** After an upgrade to Junos Space Release 14.1 or later, remote users who are not assigned to the Super Administrator or Job Administrator role can view only their own jobs on the Job Management page. They cannot view jobs triggered by other users.

7. Use the double list box to select roles for the remote profile. Select one or more roles from the Available list box. Selected roles appear in the Selected list box. Use the right arrow to move the selected roles to the Selected list box. Use the left arrow to move roles from the Selected list box back to the Available list box. You can also double-click a role to move it from one list to the other. You see the details of selected roles appear in the right pane of the page.

8. Click **Next**.

   The Domain Assignment area appears, displaying all available domains.

9. Select domains where the user can operate.

10. Click **Finish**.

    A new remote profile is added.

Remote profiles can be modified, deleted, and tagged.

NOTE: A user is not allowed to log in if the remote profile specified in the remote server does not exist in the local database. The message "No roles assigned for this user" is displayed on the login page. This information is logged in the audit log.

RELATED DOCUMENTATION

- Predefined Roles Overview | 999
- Remote Authentication Overview | 1457
- Junos Space Authentication Modes Overview | 1458
- Modifying a Remote Profile | 1100

Modifying a Remote Profile

You modify a remote profile when you want to modify the details of a remote profile.

To modify a remote profile:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **Remote Profiles**.

   The Remote Profiles page is displayed.

2. Select the remote profile that you want to modify and click the Modify Remote Profile icon on the toolbar.

   The Modify Remote Profile page is displayed.

3. (Optional) In the Role Assignment area, modify the parameters of the remote profile such as the name of the remote profile, description of the remote profile, and roles assigned to the remote profile.

4. (Optional) To modify the domains associated with the remote profile, click **Next**.

   The Domain Assignment area is displayed.

5. (Optional) Modify the domains associated with the remote profile.

6. Click **Finish**.

The remote profile is modified. You are redirected to the Remote Profiles page.

An audit log entry is generated for this task.

RELATED DOCUMENTATION

- Remote Authentication Overview | 1457
- Junos Space Authentication Modes Overview | 1458
- Creating a Remote Profile | 1098
- Deleting Remote Profiles | 1101

Deleting Remote Profiles

You delete remote profiles from Junos Space Network Management Platform when you do not need to retain the remote profiles in the database.

To delete remote profiles:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **Remote Profiles**. The Remote Profiles page is displayed.

2. Select the remote profiles that you want to delete and click the Delete icon on toolbar.

   The Delete Remote Profiles pop-up window is displayed.

3. Click **Delete**.

   The remote profiles are deleted. You are redirected to the Remote Profiles page.

   An audit log entry is generated for this task.

RELATED DOCUMENTATION

- Remote Authentication Overview | 1457
- Junos Space Authentication Modes Overview | 1458
- Creating a Remote Profile | 1098
- Modifying a Remote Profile | 1100

CHAPTER 64

API Access Profiles

IN THIS CHAPTER

- Creating an API Access Profile | 1102
- Modifying an API Access Profile | 1104
- Deleting API Access Profiles | 1105

Creating an API Access Profile

An API Access Profile restricts a Junos Space user from executing RPC commands that are potentially unsafe for or harmful to your network. An API Access Profile is a set of rules that are used to validate an RPC command executed using the **exec-rpc** API. A rule is an XPath expression (XPath 1.0). An audit log entry is generated when you create, modify, or delete an API Access Profile.

You can assign an API Access Profile to both local and remote user accounts. You assign an API Access Profile to a user when you create or modify a user account or a remote profile. For more information about creating user accounts, see "Creating Users in Junos Space Network Management Platform" on page 1035.

> **NOTE:** If an API Access Profile is not associated with a user account, the user cannot execute any RPC commands on the device. If the user tries to execute an RPC command, **Unauthorized Access Error** is displayed.

You create an API Access Profile when you need to execute RPCs by using APIs.

To create an API Access Profile:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **API Access Profiles**.

   The API Access Profiles page that appears displays the list of API Access Profiles in the Junos Space Platform database.

2. Click the Create API Access Profile icon.

The Create API Access Profile page is displayed.

3. In the **Name** field, enter a name for the new API Access Profile.

   An API Access Profile name cannot exceed 32 characters and can contain only letters, numbers, spaces, and some special characters. The special characters allowed are hyphen (-), underscore (_), and period (.). Leading and trailing spaces are not allowed. The name should start or end only with letters or numbers.

4. (Optional) In the **Description** field, enter a description for the new API Access Profile.

   The description cannot exceed 256 characters and can contain letters, numbers, spaces, and special characters.

5. On the RPC Command Rules tab, click the Add Rule icon.

   The Add/Edit Rule pop-up window is displayed. This pop-up window displays the rules that are associated with other API Access Profiles.

6. In the **Rule** drop-down list, enter the RPC command rule.

   NOTE: You can also select the rules associated with other API Access Profiles from the drop-down list.

7. Click **OK**.

   The new RPC command rule is added to the API Access Profile.

   NOTE: Repeat steps 5 through 7 to add more RPC command rules. You must add at least one rule to the API Access Profile to be able to save the profile in the Junos Space Platform database.

8. Click **Save** to save the API Access Profile.

   You are redirected to the API Access Profiles page.

NOTE: You can view the details of an API Access Profile. To do so, right-click the API Access Profile and select **View API Access Profile Detail** or double-click the API Access Profile.

RELATED DOCUMENTATION

Modifying an API Access Profile | 1104
Deleting API Access Profiles | 1105
Role-Based Access Control Overview | 995
Modifying a User | 1044

Modifying an API Access Profile

You modify an API Access Profile when you need to modify the RPC command rules in the API Access Profile.

To modify an API Access Profile:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **API Access Profiles**.

   The API Access Profiles page that appears displays the list of API Access Profiles in the Junos Space Platform database.

2. Right-click the API Access Profile you need to modify and select **Modify API Access Profile**.

   The Modify API Access Profile page is displayed.

   NOTE: You can modify all the fields of the API Access Profile except the name of the API Access Profile. For more information about modifying RPC command rules, see "Creating an API Access Profile" on page 1102.

3. Click **Save**.

   The API Access Profile is modified.

RELATED DOCUMENTATION

Creating an API Access Profile | 1102
Deleting API Access Profiles | 1105

Deleting API Access Profiles

You delete API Access Profiles when you need to remove them from the Junos Space Network Management Platform database.

To delete API Access Profiles:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **API Access Profiles**.

   The API Access Profiles page that appears displays the list of API Access Profiles in the Junos Space Platform database.

2. Right-click the API Access Profiles you need to delete and select **Delete API Access Profiles**.

   The Delete API Access Profiles pop-up window is displayed.

3. Click **Delete**.

   The API Access Profiles are deleted.

> **NOTE:** You cannot delete an API Access Profile if it is assigned to a user.

RELATED DOCUMENTATION

Creating an API Access Profile | **1102**

Modifying an API Access Profile | **1104**

CHAPTER 65

User Sessions

IN THIS CHAPTER

- User Sessions Overview | 1106
- Limiting User Sessions in Junos Space | 1108
- Terminating User Sessions | 1110
- Using the Junos Space CLI to View Users Logged In to the Junos Space GUI | 1111

User Sessions Overview

As a Junos Space User Administrator, you can view and terminate user sessions before starting a maintenance cycle to minimize the risk of system inconsistency. You can view the list of users who are logged in along with the IP address of the client from which they are logged in and the duration of their sessions. You can select one or more users to terminate their sessions.

To view the sessions of the users who are currently logged in to Junos Space Platform, on the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **User Sessions**.

Table 131 describes the column names on the User Sessions page that lists user sessions that are currently active on Junos Space Platform.

Table 131: User Sessions Page

Column Name	Description
User Name	Name of the user
Current Domain	Domain with which the user is associated
IP Address	IP address of the system from which the user has logged in
Fabric Node Name	Name of the node in the Junos Space fabric that is currently handling the user session
Session Start Time	Date and time at which the user session was initiated

Table 131: User Sessions Page *(continued)*

Column Name	Description
Session Duration	Duration of the user session

NOTE: If the node on which the user is currently logged in goes down, the name of the currently active node is displayed in the Fabric Node Name column after the switchover to the active node.

RELATED DOCUMENTATION

Terminating User Sessions | **1110**

Using the Junos Space CLI to View Users Logged In to the Junos Space GUI | **1111**

Limiting User Sessions in Junos Space

Using Junos Space Network Management Platform, you can configure the maximum number of concurrent UI sessions that are allowed for each user, both globally and at the individual user level, which can help you improve system performance.

When this limit is configured, any login attempt from the GUI is validated against this limit and the user is prevented from logging in if the concurrent user sessions limit is reached for that user. The user is notified with the following message:
You are not allowed to login since your sessions exceed the configured limit.
The audit log entry also includes the reason for login failure:
Login Failed. Maximum concurrent user session limit is reached.

In Junos Space Platform, you can configure a global concurrent UI sessions limit that is applicable to all users. However, if you have a user-level configuration limit for a specific user, then this configuration limit takes precedence over the global configuration limit for users. For example, if you set the global limit to 5 and the user-level limit to 10 for user A, then user A is prevented from logging in at the eleventh attempt. However, if the global limit is set to 10 and the user-level limit is set to 5, then the user is rejected at the sixth login attempt.

In instances where you have the same user configured locally as well as remotely (that is, on the TACACS+ or RADIUS server), the concurrent UI sessions limit that is most restrictive takes effect. For example, if you have set the sessions limit to 1 in the TACACS+ server and to 2 in Junos Space Platform for user B, then user B is prevented from logging in at the second attempt. When the sessions limit is set to 2 in the TACACS+ server and to 1 in Junos Space Platform, you can see the same results of the user being rejected at the second attempt.

> **NOTE:** The concurrent user sessions limit does not apply if you are a **super** user and you are allowed to log in even when you have exceeded this limit.

Consider the following points while setting the concurrent user sessions limit:

- Accessing the Junos Space GUI from two tabs of the same browser is considered a single session.
- Accessing the GUI from an incognito tab is considered a separate session.
- Accessing the GUI from another browser is considered a separate session.
- Configuring Junos Space parameters by using APIs is not considered a session.

This topic provides information about how to set the global limit for concurrent UI sessions per user in Junos Space Platform. For more information about setting user-level limits for concurrent UI sessions for new and existing users, see "Creating Users in Junos Space Network Management Platform" on page 1035 and "Modifying a User" on page 1044 respectively.

To set the concurrent user sessions limit globally:

1. On the Junos Space Platform UI, select **Administration > Applications**.

   The Applications page appears.

2. Select **Network Management Platform**.

3. Select **Modify Application Setting** from the Actions menu.

   The Modify Network Management Platform Settings page appears.

4. Click **User**.

5. In the **Maximum concurrent UI sessions per user** field, enter the maximum number of concurrent UI sessions that should be allowed per user.

   By default, a user is allowed up to five concurrent UI sessions. You can enter a value from 0 through 999. A value of 0 (zero) means that there is no restriction on the number of concurrent UI sessions that are allowed per user. However, the system performance may be affected if you allow unlimited sessions.

6. Click **Modify** to save the global limit for the number of concurrent UI sessions that should be allowed per user.

> **NOTE:** The changes that you make to the concurrent UI sessions limit (either at the global level or at the user level) do not affect existing sessions. That is, this limit is validated against the next user login only.

For troubleshooting, see the **/var/log/jboss/servers/server1/server.log** file, which captures internal errors. Also, see the audit logs, which capture the following information:

- Configuration changes made by the administrator to the global concurrent UI sessions limit
- The time at which the global configuration is overridden at the user level
- The time at which the concurrent UI sessions limit is reached for a user

RELATED DOCUMENTATION

Configuring Users to Manage Objects in Junos Space Overview | **1033**

Creating Users in Junos Space Network Management Platform | **1035**

Modifying a User | **1044**

Terminating User Sessions

When you trigger a session termination, the users whose sessions you have chosen for termination are notified. The notification includes the date and time when the sessions will be terminated. As a user whose session will be terminated, you are automatically logged out at the scheduled date and time and redirected to the login page.

> **NOTE:** You cannot terminate sessions of a user with the username *super*.

When you delete or disable a user in Junos Space Network Management Platform, the user's sessions is terminated automatically. If a user closes the session before the scheduled time for terminating the session and logs back in, the new session is not considered for session termination.

To terminate user sessions:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control** > **User Sessions**.

   The User Sessions page that appears displays the list of users that are currently logged in to Junos Space.

2. Select one or more users whose sessions you want to terminate.

3. Select **Terminate User Session** from the Actions menu.

   The Terminate User Session pop-up window is displayed. This page displays the user sessions that you have selected to terminate and the IP address from which the users are logged in currently.

4. Select the **Schedule at a later time** check box to terminate the user sessions at a future point in time.

5. Select the appropriate date and time for terminating sessions from the date and time menus, respectively.

6. Click **Confirm** on the Terminate User Session page.

A job is created to terminate the sessions selected for session termination. When the job is scheduled, the users whose sessions you have selected for terminating receive a pop-up message displaying the date and time you have specified for terminating their sessions.

When you terminate a user session, an audit log entry is automatically generated. On the Audit Log page (**Audit Logs** > **Audit Log**), you can filter data in the **Task** column by using the Terminate keyword to determine the number of terminated sessions, the name of the user that initiated this termination (from

the **User Name** column), the IP address from which the user session is terminated (from the **User IP** column), the time at which the session is terminated (from the **Timestamp** column), and so on.

RELATED DOCUMENTATION

Creating Users in Junos Space Network Management Platform | 1035

Predefined Roles Overview | 999

Using the Junos Space CLI to View Users Logged In to the Junos Space GUI

Junos Space administrators can execute the **jmp_users** command in the Junos Space CLI to view users logged in to the Junos Space GUI.

The command output contains the following details:

- USER NAME: Specifies the user logged in to the Junos Space GUI
- IP ADDRESS: Specifies the IP address from which the user has logged in to the Junos Space GUI
- LOGIN TIME: Specifies the time when the user logged in to the Junos Space GUI
- NODE NAME: Specifies the name of the Junos Space node to which the user has logged in or, in other words, the Junos Space node that is serving the user

To view the users logged in to the Junos Space GUI by using the Junos Space CLI:

1. Log in to the Junos Space CLI.

   The Junos Space Settings Menu appears.

2. On the Junos Space Settings Menu, to access shell, type one of the following numbers:
   - **6**, if the Junos Space Appliance is a JA2500 Junos Space hardware appliance
   - **7**, if the Junos Space Appliance is a virtual appliance

   You are prompted to enter the administrator password.

3. Enter the administrator password.

4. At the command prompt, type one of the following commands:
   - **jmp_users all** to view all the users logged in to the Junos Space fabric

     The following sample shows the output of the **jmp_users all** command:

```
+-----------+----------------+---------------------+--------------+
| USER NAME | IP ADDRESS     | LOGIN TIME          | NODE NAME    |
+-----------+----------------+---------------------+--------------+
| super     | 192.168.27.10  | 2014-12-18 8:50:02  | Node4      |
| super     | 192.168.28.11  | 2014-12-18 9:00:25  | Node4      |
| usr01     | 192.168.28.19  | 2014-12-18 10:10:10 | Node3      |
| usr02     | 192.168.29.15  | 2014-12-18 11:36:42 | Node3      |
+-----------+----------------+---------------------+--------------+
```

- **jmp_users -node *nodename*** to view the users logged in to the node specified by *nodename*; the *nodename* can be the IP address or the host name of the node

  The following sample shows the output of the **jmp_users -node Node4** command:

```
+-----------+----------------+---------------------+--------------+
| USER NAME | IP ADDRESS     | LOGIN TIME          | NODE NAME    |
+-----------+----------------+---------------------+--------------+
| super     | 192.168.27.10  | 2014-12-18 8:50:02  | Node4      |
| super     | 192.168.28.11  | 2014-12-18 9:00:25  | Node4      |
+-----------+----------------+---------------------+--------------+
```

- **jmp_users currentnode** to list the users logged in to the same node as the administrator, or in other words, served by the node to which the administrator has logged in

  You can also enter only **jmp_users**, without any options, (default option) to view the users logged in to the same node as the administrator.

  The following sample shows the output of the **jmp_users currentnode** command, where **currentnode** is Node3:

```
+-----------+----------------+---------------------+--------------+
| USER NAME | IP ADDRESS     | LOGIN TIME          | NODE NAME    |
+-----------+----------------+---------------------+--------------+
| usr01     | 192.168.28.19  | 2014-12-18 10:10:10 | Node3      |
| usr02     | 192.168.29.15  | 2014-12-18 11:36:42 | Node3      |
+-----------+----------------+---------------------+--------------+
```

RELATED DOCUMENTATION

User Sessions Overview | 1106

PART 11

Audit Logs

Overview | **1115**

Managing Audit Logs | **1117**

CHAPTER 66

Overview

IN THIS CHAPTER

- Junos Space Audit Logs Overview | 1115

Junos Space Audit Logs Overview

The Audit Logs workspace of Junos Space Network Management Platform displays the login history of and tasks initiated by a user. Through this workspace, you can track login history, device management tasks, services that were provisioned on devices, and so on. However, tasks that are not initiated by users, such as device-driven activities (for example, resynchronization of network elements), and changes made from the Junos Space CLI are not recorded in audit logs. Audit logs can be used by administrators to review events; for example, to identify which user accounts are associated with an event, to determine the chronological sequence of events—that is, what happened before and during an event, and so on.

> **NOTE:** Junos Space Platform also tracks all externally-initiated non-READ REST APIs, and login and logout APIs. In addition, if the **Record HTTP Get method** check box is selected (in the Modify Network Management Platform Settings page), then Junos Space Platform tracks externally-initiated READ APIs.

Administrators can sort and filter audit logs; for example, administrators can use audit log filtering to track the user accounts that were added on a specific date, track configuration changes across a particular type of device, view services that were provisioned on specific devices, monitor user login and logout activities over time, and so on.

> **NOTE:** To use the audit log service to monitor user requests and track changes initiated by users, you must be assigned the Audit Log Administrator role.

Junos Space Platform enables you to manage the volume of audit log data stored by purging log files from the Junos Space Platform database without archiving them or by purging log files after archiving them. When you archive logs before purging them, the archived log files are saved in a single file in compressed

comma-separated values (CSV) format (extension **.csv.gz**). Audit logs can be archived locally (on the active node in the Junos Space fabric) or to a remote server. When you archive data locally, the archived log files are saved to the **/var/lib/mysql/archive** directory on the active Junos Space node.

You can schedule the purging of audit logs (with or without prior archiving) for a later date and schedule the purging on a recurring basis.

Junos Space Platform also enables you to download audit logs in CSV format so that you can view the audit logs in a separate application or save them on another machine for further use, without purging them from the system.

You can also forward audit logs to a system log server by using one or more audit log forwarding criteria.

Audit log forwarding criteria can be configured and managed from the Audit Log Forwarding page under the Administration workspace. For more information about audit log forwarding, see "Audit Log Forwarding in Junos Space Overview" on page 1492.

RELATED DOCUMENTATION

Archiving and Purging or Only Purging Audit Logs | **1126**

Viewing Audit Logs | **1117**

Exporting Audit Logs | **1123**

CHAPTER 67

Managing Audit Logs

IN THIS CHAPTER

- Viewing Audit Logs | **1117**
- Viewing Audit Log Statistics | **1121**
- Exporting Audit Logs | **1123**
- Converting the Junos Space Audit Log File Timestamp from UTC to Local Time Using Microsoft Excel | **1125**
- Archiving and Purging or Only Purging Audit Logs | **1126**

Viewing Audit Logs

Audit logs are generated for login activity and tasks that are initiated (by users) from the Junos Space Network Management Platform and Services Activation Director, as well as Service Automation.

NOTE: To view audit logs, you must have Audit Log Administrator privileges.

To view audit logs:

1. On the Junos Space Network Management Platform UI, select **Audit Logs** > **Audit Log**.

   The Audit Log page appears displaying the audit logs in tabular format. The fields displayed on the Audit Log page are described in Table 132.

2. (Optional) Click an audit log entry to view the details for that audit log.

   The Audit Log Detail dialog box is displayed. This page displays additional fields that are not displayed on the Audit Log page; these fields are described in Table 132.

   Click **OK** to close the Audit Log Detail dialog box.

3. (Optional) If the audit log entry includes a link to the job ID, click the link to display information about the job associated with the audit log entry.

   The Job List page is displayed; the fields displayed in this page are described in Table 133.

Click **Back** to go to the Audit Log page.

Table 132: Fields on the Audit Log Page and Audit Log Detail Dialog Box

Field	Description	Displayed In
ID	Audit Log ID	Audit Log page
User Name	Username of the user that initiated the task	Audit Log page Audit Log Detail dialog box
User IP	IP address of the client computer from which the user initiated the task	Audit Log page Audit Log Detail dialog box
Domain	Domain from which a user has initiated jobs	Audit Log page
Application	Name of the application from which the user initiated the task	Audit Log page Audit Log Detail dialog box
Workspace	Name of the workspace from which the user initiated the task	Audit Log Detail dialog box
Task	Name of the task that triggered the audit log	Audit Log page Audit Log Detail dialog box
Timestamp	Timestamp for the audit log file that is stored in UTC time in the database but mapped to the local time zone of the client computer.	Audit Log page Audit Log Detail dialog box
Result	Result of the task that triggered the audit log: • **Success**—Job is completed successfully. • **Failure**—Job failed and is terminated. • **Job Scheduled**—Job is scheduled but has not yet started. • **Recurring Job Scheduled**—Job scheduled with recurrence.	Audit Log page Audit Log Detail dialog box
Job ID	ID of the job-based task. As explained in the procedure, click the job ID to view detailed information about the job.	Audit Log page Audit Log Detail dialog box

Table 132: Fields on the Audit Log Page and Audit Log Detail Dialog Box *(continued)*

Field	Description	Displayed In
Description	Description of the audit log Junos Space provides additional information such as configlet name and the device name in the audit log for the following tasks that are performed via REST API: • Apply CLI Configlet • Validate CLI Configlet For example, Apply CLI Configlet/Validate CLI Configlet operation initiated for the configlet <configlet_name> on the device <device_name>.	Audit Log page Audit Log Detail dialog box
Affected Objects	Junos Space objects pertaining to the task in the audit log	Audit Log Detail dialog box
Affected Object Detail	Details about the affected Junos Space objects; for example, the information related to the Modify Application settings task	Audit Log Detail dialog box
View Configuration Detail	Details of the device configuration changes are displayed in the Configuration Details dialog box.	Audit Log Detail dialog box

NOTE: The **View Configuration Detail** link is visible on the Audit Log Detail dialog box for only the following audit log tasks: modifying device configuration, deploying device configuration, executing scripts, modifying authentication on devices, deploying templates, applying CLI configlet, deploying device image, restoring configuration, and resolving key conflicts.

Table 133: Fields on the Job List Page

Field	Description
Name	Name of the job
Job ID	Numerical ID of the job
Percent	Percentage of job that is completed

Table 133: Fields on the Job List Page *(continued)*

Field	Description
State	State of job execution: • **SUCCESS**—Job is completed successfully. • **FAILURE**—Job failed and is terminated. • **IN PROGRESS**—Job is in progress. • **CANCELED**—Job is canceled by the user.
Job Type	Type of job; for example, Discover Network Elements
Summary	Summary of the job
Scheduled Start Time	Date and time at which the job is scheduled (specified by a Junos Space user)
Actual Start Time	Date and time at which the job actually started
End Time	Date and time at which the job ended
Recurrence	Job recurrence interval, start time, and end time

Release History Table

Release	Description
16.1R1	The **View Configuration Detail** link is visible on the Audit Log Detail dialog box for only the following audit log tasks: modifying device configuration, deploying device configuration, executing scripts, modifying authentication on devices, deploying templates, applying CLI configlet, deploying device image, restoring configuration, and resolving key conflicts.

RELATED DOCUMENTATION

Exporting Audit Logs | **1123**

Viewing Audit Log Statistics | **1121**

Junos Space Audit Logs Overview | **1115**

Archiving and Purging or Only Purging Audit Logs | **1126**

Viewing Audit Log Statistics

IN THIS SECTION

- Viewing the Dynamic Audit Log Statistical Graph | **1121**
- Viewing the Top 10 Active Users In 24 Hours Statistics | **1123**

The Audit Logs workspace statistics page provides two graphs: **Audit Log Statistical Graph** pie chart and the **Top 10 Active Users in 24 Hours** graph. The audit log administrator uses these graphs to monitor the Junos Space Network Management Platform tasks.

The Audit Log Statistical Graph pie chart displays all tasks that are performed and logged in all Junos Space applications over a specific period of time. You can view Audit Log statistics by task type, user, workspace, and application.

The Top 10 Active Users in 24 hours graph displays the top ten Junos Space Network Management Platform users who performed the most number of tasks over 24 hours. The x-axis represents activities that are performed by a single user. Each active session for that user is represented by a bubble on the x-axis. The y-axis represents hours. For example, if a single user performed six active sessions during the last 24 hours, the chart displays six bubbles on the x-axis according to the hours displayed on the y-axis.

This topic contains the following sections:

Viewing the Dynamic Audit Log Statistical Graph

With the Audit Log Statistical Graph, the audit log administrator can view audit logs by selecting both category and time frame. The category—task, user, workarea, or application—determines the statistical graph that is displayed. Each slice in the pie represents a task and its usage percentage. The tasks types are listed in a box at the right of the pie chart. Mouse over a slice of the pie to see the number of times that the task is invoked. The time frame specifies the period of time within which to show audit log data.

To use the Audit Log Statistical Graph:

1. On the Junos Space Network Management Platform user interface, select **Audit Logs**.

   The Audit Logs page appears, which displays Audit Log Statistical Graph and Top 10 Active Users in 24 Hours graph.

2. On the Audit Log Statistical Graph, select a graph category:

- **Task**—Displays all tasks that are performed. Click each task slice to go to the next-level chart that displays users who performed the selected task. For example, when you click the “Login” slice, you can view the login activity (or task) of all users for the selected time frame.

  The graph path indicates where you are located in the GUI. In this example, the GUI displays Overview -> Login as the graph path. Click **Overview** to go back to the top-level chart. The task name in the path indicates the currently selected path.

  The graph pertaining to a task is displayed with a username or IP address.

  - **User Names**—By default, displays all users who performed the specific task. Click a user to go to the inventory page filtered by task, user, and selected time frame.
  - **IP Addresses**—Displays all IP addresses where users performed the specific task. Click an IP address to go to the inventory page filtered by task, IP address, and selected time frame.

- **User**—Displays all users using the system within the time frame. Ten users are displayed per chart. Click Others to go to the next page. Click the previous page link to go back.
- **Workspace**—Displays all workspaces accessed in the time frame. Click a workspace slice to go to the inventory page filtered by workspaces.
- **Application**—Displays all applications used. Click a pie slice to go to the inventory page filtered by application and selected time frame.

3. Select a time frame in days, weeks, or months to display audit log data in the pie chart for that time period. The default is Days. A time selection description is displayed below the time frame area.

   - **Days**—Displays seven days prior to the selected date. Select single or multiple days. Select multiple days by dragging the cursor along the displayed timeframe.
   - **Weeks**—Displays the past five weeks, from past to most current on the right. Select multiple days by dragging the cursor along the displayed timeframe.
   - **Months**—Displays the past 12 months, from past to most current on the right. Select multiple days by dragging the cursor along the displayed timeframe.

   The current day, week, or month is highlighted (or selected) by default.

4. Click a slice in the pie chart to view more detailed information. Tasks appear in tabular view by username, user IP address, task, timestamp, results, description, job ID, and level 2 description.

   See “Junos Space User Interface Overview” on page 89 in the *Junos Space User Interface Guide* for more information about manipulating the table data.

5. On the inventory page, double-click an audit log to view more detailed information. For a job-related log entry, click the link in the Job ID column to view a new table that shows the corresponding job information.

In the audit log detail view, if there are multiple affected objects for a log entry, the affected object detail always shows the first object detail. Click any object on the list to change the object detail. If no affected object exists for this log entry, the affected object list is hidden and no object detail is displayed.

6. Click Return to Audit Logs to go back to Audit Log View.

Viewing the Top 10 Active Users In 24 Hours Statistics

To view the jobs performed by a user in the Top 10 Active Users in 24 Hours graph:

1. In the Top 10 Active Users in 24 Hours graph, double-click a user's bubble for a particular hour. The View Audit Log page displays the jobs performed by that user.

   Jobs appear by audit log ID, username, user IP address, domain, application, task, timestamp, results, description, and job ID in tabular view. See "Junos Space User Interface Overview" on page 89 in the *Junos Space User Interface Guide* for more information about manipulating the table data.

RELATED DOCUMENTATION

Viewing Audit Logs | **1117**

Junos Space Audit Logs Overview | **1115**

Archiving and Purging or Only Purging Audit Logs | **1126**

Exporting Audit Logs | **1123**

Exporting Audit Logs

You can export audit logs, as a comma-separated values (CSV) file, without purging the logs from the database.

To export audit logs:

1. On the Junos Space Network Management Platform UI, select **Audit Logs > Audit Log**.

   The Audit Log page appears.

2. Click the **Export Audit Logs** icon.

   The Export Audit Logs page appears.

3. Choose one of the following export actions:

- To export all logs, select **Export all audit logs**.

  The Date and Time selectors are disabled when you select this option.

- To export all logs that are currently displayed on the Audit Log page, which is the default option, select **Export audit logs currently displayed in View Audit Logs table**.

  > **NOTE:** On the Audit Log page, you can filter audit logs by using different criteria. The filtering criteria determines which audit log entries are displayed, and only those entries are exported.

- To export logs within a specific duration:

  a. Select **Export audit logs filtered by date range**.

  b. Specify the date and time from which you want to export the logs in the **Start date and time** field.

  c. Specify the date and time up to which you want to export the logs in the **End date and time** field.

4. (Optional) Select the **Include Affected Object Column** check box to include the details of the Junos Space Platform objects that are affected by the tasks logged. These tasks are listed as a column named **Affected Objects** in the audit log file.

5. Click **Export**.

   You are taken to the Audit Log page and the Exporting Audit Logs dialog box appears indicating the status of the export.

6. After the audit log is exported (status bar displays 100%), click **OK** to close the dialog box.

   The audit log file is saved to the default downloads folder of the browser.

RELATED DOCUMENTATION

Junos Space Audit Logs Overview | **1115**

Viewing Audit Log Statistics | **1121**

Archiving and Purging or Only Purging Audit Logs | **1126**

Converting the Junos Space Audit Log File Timestamp from UTC to Local Time Using Microsoft Excel

You can unzip the compressed comma-separated values (CSV) audit log file (extension **.csv.gz**) and open the extracted CSV file as a spreadsheet in Microsoft Excel. In Microsoft Excel, you can convert the entries in the Timestamp column from UTC (GMT) to local time.

To convert UTC time to local time:

1. Retrieve the audit log file from where you archived it. If you archived the file locally, the file is located in **/var/lib/mysql/archive** on the active node.

2. Unzip the audit log file (extension **.csv.gz**).

3. Open the unzipped audit log file (extension **.csv**) in Microsoft Excel.

4. To the left of the UTC Time column, insert a new column.

5. Label the column header **Local Time**.

6. Click the first cell of the new column and insert the following formula =*XX*/ 86400000 + 25569 - *Y*/24 in the cell, where *XX* represents the cell letter and row number where you want to insert the local time-conversion function and *Y* represents the difference in hours between your local time and the UTC time.

7. Press **Enter**.

   The calculated local time appears in the cell.

8. Format the local time by right-clicking the cell and selecting **Format Cells**.

   The Format Cells dialog box appears.

9. From the **Category** list, select **Date**.

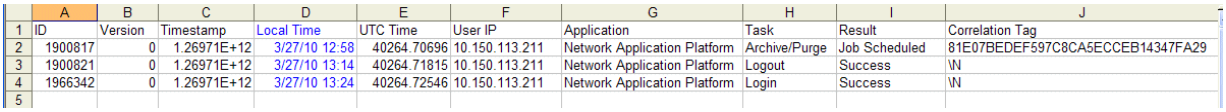
10. From the **Type** list, select a date format that you want.

11. Click **OK**.

    The local time and date are displayed in the specified format.

12. Copy or apply the cell function and formatting to the rest of the rows in the Local Time column. The rest of the local times appear as shown Figure 48.

Figure 48: Formatting the Local Times Column in Microsoft Excel



	A	B	C	D	E	F	G	H	I	J
1	ID	Version	Timestamp	Local Time	UTC Time	User IP	Application	Task	Result	Correlation Tag
2	1900817	0	1.26971E+12	3/27/10 12:58	40264.70696	10.150.113.211	Network Application Platform	Archive/Purge	Job Scheduled	81E07BEDEF597C8CA5ECCEB14347FA29
3	1900821	0	1.26971E+12	3/27/10 13:14	40264.71815	10.150.113.211	Network Application Platform	Logout	Success	\N
4	1966342	0	1.26971E+12	3/27/10 13:24	40264.72546	10.150.113.211	Network Application Platform	Login	Success	\N
5										

13. Save the Microsoft Excel file.

RELATED DOCUMENTATION

Archiving and Purging or Only Purging Audit Logs | **1126**

Archiving and Purging or Only Purging Audit Logs

IN THIS SECTION

- Purging Audit Logs Without Archiving | **1127**
- Purging Audit Logs After Archiving | **1130**

The Archive/Purge Logs page enables you to purge audit logs without archiving them or to purge audit logs after archiving them. You can purge audit logs before a specified date and time or audit logs that are older than a specified number of days. Audit logs can be archived locally (on any node that is in the **UP** state) or to a remote server.

NOTE: If more than one Archive/Purge job is scheduled at the same time, then the job that is executed first goes through and the other jobs fail. Scheduled jobs can be rescheduled from the Job Management page.

This topic includes the following sections:

Purging Audit Logs Without Archiving

To purge audit logs without archiving them:

1. On the Junos Space Network Management Platform UI, select **Audit Logs** > **Audit Log** > **Archive/Purge Logs**.

   You are taken to the Archive/Purge Logs page.

2. Using the **Purge Logs** field, specify a date and time before which audit logs should be purged or that audit logs that are older than a specified number of days should be purged:

   - To purge audit logs before a specified date and time:

     a. Select **Before**, which is the default.

     b. Enter a date in the text box (in DD/MM/YYYY format) or click the calendar icon and select a date; for example, 20/11/2014.

     c. Enter a time in the text box (in HH:MM AM/PM format) or click the down arrow icon and select a time; for example: 1:15 AM.

     > **NOTE:** You specify the time in the local time zone of the client computer but the audit logs are purged according to the time zone configured on the Junos Space Platform server.

   - To purge audit logs older than a specified number of days:

     a. Select **Older than**.

     b. Specify the number of days (the default is 90 days) such that the audit logs older than the specified number of days will be purged

3. To purge audit logs from all domains to which you have access, select the **Purge audit logs from all accessible domains** check box.

   > **NOTE:** By default, audit logs are purged only from domain that you accessed, so the **Purge audit logs from all accessible domains** check box is cleared.

4. Clear the **Archive Logs Before Purge** check box, which is selected by default.

> **CAUTION:** If you choose not to archive the audit logs before purging, the audit logs are deleted from the Junos Space Platform database and cannot be recovered.

5. (Optional) To schedule the purge operation for later, select the **Schedule at a later time** check box and specify a start date and time for the purge.

   > **NOTE:** You specify the time in the local time zone of the client computer but the purge is scheduled according to the time zone configured on the Junos Space Platform server.

6. (Optional) To specify whether the purge should be done on a recurring basis, select the **Recurrence** check box.

   > **NOTE:** This option is enabled only if you choose to purge audit logs older than a specified number of days.

   A number of fields allowing you to specify when the purge should recur are displayed. The fields are explained in Table 134.

   Table 134: Fields for Specifying Recurring Purges

Field Name	Description
Repeats	Specify the periodicity of the recurrence: • **Minutes** • **Hourly** • **Daily** • **Weekly** • **Monthly** • **Yearly**
Repeat every	Specify the period at which the purge should recur. For example, if you specified a periodicity in hours (**Hourly**), enter the number of hours after which the purge should recur.

Table 134: Fields for Specifying Recurring Purges *(continued)*

Field Name	Description
Repeat by	Specify one or more days on which you want the purge to recur. **NOTE:** • This field is displayed only when you specify a weekly periodicity (**Weekly**). • The *day* on which the purge is scheduled is disabled. For example, if you scheduled a job on a Wednesday, then **Wed** is selected by default and disabled. You can select other days by enabling the corresponding check boxes.
Ends	Specify one of the following: • Select **Never** to continue (without an end date) the recurring purge operation at the specified recurrence interval. • Select **On** and specify a date and time on which to stop the recurring purge operation.

7. Click **Submit**.

   Junos Space Platform checks whether a job of this type already exists for that domain:

   - If a job already exists, then a message is displayed indicating that conflicting jobs exist, and the existing conflicting jobs are displayed in a table.

     a. Click **Yes** to create a new job.

        The Audit Log Archive/Purge confirmation dialog box is displayed with the audit log archive filename and location and a warning indicating that the audit logs will be purged from the database.

     b. Click **No** to return to the previous page.

        You are taken to the previous page.

   - If no job exists, then the Audit Log Archive/Purge confirmation dialog box is displayed with the audit log archive filename and location and a warning indicating that the audit logs will be purged from the database.

8. In the Audit Log Archive/Purge dialog box, click **Continue** to archive and purge the logs.

   The Job Information dialog box is displayed with the job ID. Click the *Job ID* to view the details; otherwise, click **OK** to close the dialog box.

Purging Audit Logs After Archiving

To purge audit logs after archiving them:

1. On the Junos Space Network Management Platform UI, select **Audit Logs** > **Audit Log** > **Archive/Purge Logs**.

   You are taken to the Archive/Purge Logs page.

2. Using the **Purge Logs** field, specify a date and time before which audit logs should be archived and purged or that audit logs that are older than a specified number of days should be archived and purged:

   - To archive and purge audit logs before a specified date and time:

     a. Select **Before**, which is the default.

     b. Enter a date in the text box (in DD/MM/YYYY format) or click the calendar icon and select a date; for example, 20/11/2014.

     c. Enter a time in the text box (in HH:MM AM/PM format) or click the down arrow icon and select a time; for example: 1:15 AM.

     > **NOTE:** You specify the time in the local time zone of the client computer but the audit logs are archived and purged according to the time zone configured on the Junos Space Platform server.

     > **NOTE:** In this case, the format of the audit log filename is **JunosSpaceAuditLog_*purge-date-and-time*_*date-and-time-in-ms*.csv.gz**, where *purge-date-and-time* is the specified purge date (in *yyyy-mm-dd* format) and time (in *hh-mm-ss* format), and *date-and-time-in-ms* is the date and time in milliseconds at which the job was created.

   - To archive and purge audit logs older than a specified number of days:

     a. Select **Older than**.

     b. Specify the number of days (the default is 90 days) such that the audit logs older than the specified number of days will be archived and purged

> **NOTE:** In this case, the format of the audit log filename is **JunosSpaceAuditLog_*purge-after-days_date-and-time_date-and-time-in-ms*.csv.gz**, where *purge-after-days* is the previously specified number of days, *date-and-time* is the date (in *yyyy-mm-dd* format) and time (in *hh-mm-ss* format) before which audit logs will be purged, and *date-and-time-in-ms* is the date and time in milliseconds at which the job was created.

3. To archive and purge audit logs from all domains to which you have access, select the **Purge audit logs from all accessible domains** check box.

   > **NOTE:** By default, audit logs are archived and purged only from domain that you accessed, so the **Purge audit logs from all accessible domains** check box is cleared.

4. Select the **Archive Logs Before Purge** check box.

5. Specify whether you want to archive the files locally or on a remote server:
   - To archive the files locally (on the active node), from the **Archive Mode** list, select **local**.
   - To archive the files on a remote server:
     a. From the **Archive Mode** list, select **remote**.
     b. In the **User** field, enter a valid username to access the remote server.
     c. In the **Password** field, enter a valid password to access the remote server.
     d. In the **Confirm Password** field, reenter the password you entered in the preceding step.
     e. In the **Machine IP** field, enter the IP address of the remote server.

NOTE:

- Depending on whether the Junos Space fabric is configured with only IPv4 addresses or both IPv4 and IPv6 addresses, Junos Space Platform allows you to enter an IPv4 address or either an IPv4 or IPv6 address respectively for the remote server.
- The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to http://www.iana.org/assignments/ipv4-address-space for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space for the list of restricted IPv6 addresses.

f. In the **Directory** field, enter the directory path on the remote server on which to store the archived log files, ensuring that the directory name ends with /; for example, **/home/spaceauditlogs/**.

NOTE: The directory must already exist on the remote server.

6. (Optional) To schedule the archive and purge operation for later, select the **Schedule at a later time** check box and specify a start date and time for the archive and purge operation.

NOTE: You specify the time in the local time zone of the client computer but the archive and purge operation is scheduled according to the time zone configured on the Junos Space Platform server.

7. (Optional) To specify whether the archive and purge should done on a recurring basis, select the **Recurrence** check box.

NOTE: This option is enabled only if you choose to archive and purge audit logs older than a specified number of days.

A number of fields allowing you to specify when the archive and purge should recur are displayed. The fields are explained in Table 134.

8. Click **Submit**.

Junos Space Platform checks whether a job of this type already exists for that domain:

- If a job already exists, then a message is displayed indicating that conflicting jobs exist, and the existing conflicting jobs are displayed in a table.

  a. Click **Yes** to create a new job.

     The Audit Log Archive/Purge confirmation dialog box is displayed with the audit log archive filename and location and a warning indicating that the audit logs will be purged from the database.

  b. Click **No** to return to the previous page.

     You are taken to the previous page.

- If no job exists, then the Audit Log Archive/Purge confirmation dialog box is displayed with the audit log archive filename and location and a warning indicating that the audit logs will be purged from the database.

9. In the Audit Log Archive/Purge dialog box, click **Continue** to archive and purge the logs.

   The Job Information dialog box is displayed with the job ID. Click the *Job ID* to view the details; otherwise, click **OK** to close the dialog box.

RELATED DOCUMENTATION

Junos Space Audit Logs Overview | **1115**

Viewing Audit Logs | **1117**

Exporting Audit Logs | **1123**

PART 12

Administration

Overview | **1136**

Managing Nodes in the Junos Space Fabric | **1156**

Backing up and Restoring the Junos Space Platform Database | **1304**

Managing Licenses | **1323**

Managing Junos Space Platform and Applications | **1328**

Managing Troubleshooting Log Files | **1408**

Managing Certificates | **1426**

Configuring Authentication Servers | **1457**

Managing SMTP Servers | **1477**

Email Listeners | **1481**

Managing Git Repositories | **1485**

Audit Log Forwarding | **1492**

Configuring a Proxy Server | **1502**

Managing Tags | **1505**

Managing DMI Schemas | **1534**

Managing Hardware Catalog | **1559**

Managing the Purging Policy | **1566**

CHAPTER 68

Overview

IN THIS CHAPTER

- Junos Space Administrators Overview | 1136
- Viewing the Administration Statistics | 1138
- Junos Space IPv6 Support Overview | 1152
- Maintenance Mode Overview | 1153

Junos Space Administrators Overview

Junos Space administrators serve different functional roles. A CLI administrator installs and configures Junos Space Appliances. A maintenance-mode administrator performs system-level tasks, such as troubleshooting and database restore operations. After Junos Space Appliances are installed and configured, users created from the Junos Space user interface perform the roles of accessing workspaces and managing applications, users, devices, services, customers, and so forth. Typically, an administrator performs most of the tasks from the Administration workspace. This entire workspace is available only if you are working in the global domain. You can identify the domain that you are currently in from the banner on the Junos Space Network Management Platform user interface. In subdomains, only the tags task is available under the Administration workspace.

Table 135 describes Junos Space administrators and Junos Space user UI users and the tasks that they perform.

Table 135: Junos Space Administrators and Junos Space UI Users

Junos Space Administrator	Description	Tasks

Table 135: Junos Space Administrators and Junos Space UI Users *(continued)*

CLI administrator	An administrator responsible for setting up and managing the system settings for Junos Space Appliances from the serial console.
	
	The CLI administrator name is “admin.”
	
	The CLI administrator password can be changed from the console system settings menu.
		• Install and configure basic settings for Junos Space Appliances.
		• Change network and system settings for Junos Space appliances, for example:
		  ◦ Change the CLI administrator password.
		  ◦ Change network settings, such as:
		  ▪ Set DNS servers.
		  ▪ Change IP address of the Junos Space node.
		  ▪ Change static routes.
		  ◦ Change time options.
		  ◦ Expand VM drive size (Junos Space Virtual Appliances only).
		
		NOTE: This option is available only if the Junos Space node is running on a virtual machine (VM).
		
		  ◦ Retrieve log files for troubleshooting.
		  ◦ Update the security settings, such as disable firewall or SSH
		  ◦ Debug

Maintenance-mode administrator	An administrator responsible for performing system-level maintenance on Junos Space Platform. The maintenance-mode administrator name is “maintenance.” You can configure the maintenance-mode password is through the serial console when you first configure a Junos Space Appliance.	• Restore Junos Space Platform to its previous state by using a database backup file. • Shut down Junos Space nodes by entering maintenance mode. • Retrieve log files for troubleshooting. • Exit maintenance mode and explicitly start up the Junos Space Platform.

Table 135: Junos Space Administrators and Junos Space UI Users *(continued)*

Junos Space user interface users	A Junos Space user that is assigned one or more predefined roles. Each role assigned to a user provides specific access and management privileges on the objects (applications, devices, users, jobs, services, customers, and so on) available from a workspace on the Junos Space user interface.	For complete information about predefined roles that can be assigned to a Junos Space user, see "Predefined Roles Overview" on page 999.

NOTE:

- Junos Space allows only admin user login for Space server CLI access. Its not recommended to create custom SSH user for Junos Space CLI access.
- Juniper Networks devices require a license to activate the feature. To understand more about Junos Space Network Management Platform Licenses, see, Licenses for Network Management. Please refer to the Licensing Guide for general information about License Management. Please refer to the product Data Sheets for further details, or contact your Juniper Account Team or Juniper Partner.

RELATED DOCUMENTATION

Maintenance Mode Overview | **1153**

Role-Based Access Control Overview | **995**

Configuring Users to Manage Objects in Junos Space Overview | **1033**

Viewing the Administration Statistics

IN THIS SECTION

- Viewing System Health Information | **1139**
- Viewing the System Health Report | **1139**
- Viewing System Alert Messages in the Last 30 Days | **1150**

The Administration statistics page displays the following information: graphical details about system health; a system health report on the Junos Space fabric, and JBoss and MySQL database processes; and a list of system alert messages that were received in the last 30 days.

To access the Administration statistics page:

1. On the Junos Space Network Management Platform UI, select **Administration**.

   The Administration statistics page appears, displaying three boxes titled **System Health**, **System Health Report**, and **System Alert Messages in Last 30 Days**.

This topic contains the following sections:

Viewing System Health Information

The **System Health** section displays three charts related to system health. For more information about these charts, see "Viewing the Junos Space Platform Dashboard" on page 126.

Viewing the System Health Report

Starting with Junos Space Network Management Platform Release 15.2R1, you can view records about the health and performance of the Junos Space nodes in your Junos Space setup and the processes on these nodes in a system health report. The health and performance data collected from the nodes is displayed in a table. The health and performance data is categorized by parameters related to the Junos Space fabric and the JBoss and MySQL processes.

The Process column in the table displays the process and the Parameter column displays the parameter of the process that is evaluated. The Status column displays the status of the parameter. *No* is displayed in green if the parameter is within the configured threshold. *Yes* is displayed in red to indicate that the process has exceeded the threshold and must be corrected by the administrator. The Status column displays *Yes* in red until the issue is fixed. A user assigned with appropriate privileges can click the **Click** link corresponding to the process in the More Details column to view more details.

Table 136 lists the processes, parameters, descriptions, and data displayed when you click the links in the More Details column, and the type of nodes from which the parameter collects the system health details.

You can configure appropriate threshold values and time intervals to collect health and performance data and update the System Health Report. These thresholds are applicable to all relevant nodes in the Junos Space fabric. For more information about configuring thresholds and time intervals, see the *Health Monitoring* section in the "Modifying Junos Space Network Management Platform Settings" on page 1346 topic.

NOTE: You must be assigned the privileges of a Super Administrator, System Administrator, or any role with appropriate privileges to view more details by clicking the link related to the process and parameter.

To alert selected users and fix issues when the parameter exceeds the threshold, you can add users to the Email Listeners list to receive notifications. Users receive e-mail alerts when the health and performance of the Junos Space nodes are below the threshold and the Status column displays *Yes* in red. For more information about adding users, see "Adding Users to the Email Listeners List" on page 1482.

NOTE: The Multi-Master Detected and MySQL in out of sync state parameters display N/A in a single-node Junos Space setup.

NOTE: The Fabric node in the DOWN state detected parameter and the JGroups membership issue detected parameter are displayed only in a Junos Space setup with multiple JBoss nodes.

Table 136: System Health Report: Processes and Parameters

Process Name	Parameter Name	Description	Data Displayed on Clicking the Links	Applicable Node Types
Fabric	CPU counters are inactive	This parameter detects whether the time interval (specified in the **Interval for monitoring CPU counters update in minutes** field on the Modify Application Settings page) has elapsed (with system time as the reference) from the time that the overall load on a Junos Space node and CPU resources shared by the processes on the node is calculated. The default is two minutes.	You are directed to the **Administration > Fabric** page with a filtered view of the nodes that match the parameter criteria. See Table 137 for the details displayed on the page. View the Last Update Time column on this page.	JBoss, database, FMPM, and Log collector

Table 136: System Health Report: Processes and Parameters *(continued)*

Process Name	Parameter Name	Description	Data Displayed on Clicking the Links	Applicable Node Types
Fabric	Disk utilization is abnormal	This parameter collects information about hard-drive utilization (displayed as a percentage) in the / directory on a Junos Space node in the fabric. The default is 50%.	You are directed to the **Administration > Fabric** page with a filtered view of the nodes that match the parameter criteria. View the %Disk column on this page.	JBoss, database, FMPM, and Log collector
Fabric	High CPU detected in last 3 days	This parameter detects whether the CPU usage on a Junos Space node has exceeded the configured threshold (default: 50%) for a duration called Extended Period (default: 30 minutes). The threshold can be specified in the **High CPU Threshold Value in percentage** setting and the duration can be specified in the **Extended Period for High CPU in minutes** field on the Modify Application Settings page. The default is 50%.	You are directed to the **Administration > Fabric > Extended Periods of High CPU** page. See Table 137 for the details displayed on the page. Click **Close** to return to the Administration statistics page.	JBoss, database, FMPM, and Log collector
Fabric	Processes are running incorrectly	This parameter detects processes such as JBoss, MySQL, Apache Web Proxy, OpenNMS, and PostgreSQL that are in the DOWN status on a Junos Space node.	You are directed to the **Administration > Fabric** page with a filtered view of the nodes that match the parameter criteria. Right-click a node and select **View Fabric Node Details**, or double-click inside a row corresponding to a node and click the Process Detail tab, to view the processes that are running incorrectly.	JBoss, database, FMPM, and Log collector **NOTE:** On the FMPM node, only the OpenNMS process is monitored.

Table 136: System Health Report: Processes and Parameters *(continued)*

Process Name	Parameter Name	Description	Data Displayed on Clicking the Links	Applicable Node Types
Fabric	Management sessions are mismatched with UI data	This parameter detects a difference between the number of device management SSH sessions calculated on each Junos Space node by the **netstat -anlp | awk '{print $5}' | grep ":22" | wc –l** command and the number of device management SSH sessions as per the Junos Space database. This parameter displays *Yes* in red only if the difference exceeds the tolerance specified in the **Device Management Sessions Monitoring Threshold** setting on the Modify Application Settings page. **NOTE:** If you configured a different port number for the SSH device connection, the parameter uses the modified SSH port in the **netstat** command. The default is 10.	You are directed to the **Administration > Fabric > Device Management Sessions** page with a list of nodes that match the parameter criteria. See Table 138 for the details displayed on the page. Click **Close** to return to the Administration statistics page.	JBoss
Fabric	MySQL in out of sync state	This parameter detects a MySQL database synchronization issue between nodes running the MySQL database (Database column displays Out-of-Sync).	You are directed to the **Administration > Fabric** page with a filtered view of the nodes running the MySQL database. View the Database column on this page.	Database

Table 136: System Health Report: Processes and Parameters *(continued)*

Process Name	Parameter Name	Description	Data Displayed on Clicking the Links	Applicable Node Types
Fabric	VIP Bind issue detected in JBoss node(s)	This parameter detects the assignment of the VIP address to multiple JBoss nodes or to no JBoss node in the Junos Space fabric. The status of the node is displayed in the Load Balancer column as *UP*, *DOWN*, *Standby*, *Unknown*, or *N/A*. **NOTE:** On detection and on resolution of an issue, a trap is raised and an e-mail is sent to the Email Listeners list.	You are directed to the **Administration > Fabric** page with a filtered view of the load-balancer nodes. View the Load Balancer column on this page.	JBoss
Fabric	VIP Bind issue detected in DB nodes(s)	This parameter detects the assignment of the VIP address to multiple database nodes or to no database node in the Junos Space fabric. The status of the node is displayed in the Database column as *UP*, *DOWN*, *Standby*, *Unknown*, or *N/A*. **NOTE:** On detection and on resolution of an issue, a trap is raised and an e-mail is sent to the Email Listeners list.	You are directed to the **Administration > Fabric** page with a filtered view of the database nodes. View the Database column on this page.	Database
Fabric	VIP Bind issue detected in FMPM nodes(s)	This parameter detects the assignment of the VIP address to multiple FMPM nodes or to no FMPM node in the Junos Space fabric. The status of the node is displayed in the App Logic column as *UP*, *DOWN*, *Standby*, *Unknown*, or *N/A*. **NOTE:** On detection and on resolution of an issue, a trap is raised and an e-mail is sent to the Email Listeners list.	You are directed to the **Administration > Fabric** page with a filtered view of the FMPM nodes. View the App Logic column on this page.	FMPM

Table 136: System Health Report: Processes and Parameters *(continued)*

Process Name	Parameter Name	Description	Data Displayed on Clicking the Links	Applicable Node Types
Fabric	Fabric node in the DOWN state detected	This parameter detects one or more nodes in the Junos Space fabric in the DOWN state. **NOTE:** On detection and on resolution of an issue, a trap is raised and an e-mail is sent to the Email Listeners list.	You are directed to **Administration > Fabric** page with a filtered view of the fabric nodes in the DOWN state.	JBoss, database, FMPM, and Log collector
Fabric	JGroups membership issue detected	This parameter detects the removal of a JBoss node in the cluster. **NOTE:** On detection and on resolution of an issue, a trap is raised and an e-mail is sent to the Email Listeners list.	You are directed to **Administration > Fabric** page with a filtered view of JBoss nodes in the JGroups membership set.	JBoss
Fabric	File Integrity Check Failed	This parameter detects any breach in	You are directed to **Administration > Fabric** page with a filtered view of the node on which the file integrity check failed.	JBoss, database, and FMPM
JBoss	JBoss restart observed in last 3 days	This parameter logs the time when JBoss was restarted on a node during the last three days.	You are directed to the **Administration > Fabric > Last JBoss Restarted Time** page. See Table 140 for the details displayed on the page. Click **Close** to return to the Administration statistics page.	JBoss
JBoss	Multi-Master detected (App Logic)	This parameter detects and reports the presence of multiple fabric nodes running as the JBoss primary node.	You are directed to the **Administration > Fabric** page with a filtered view of multiple primary nodes in the Junos Space fabric. View the App Logic column on this page.	JBoss

Table 136: System Health Report: Processes and Parameters *(continued)*

Process Name	Parameter Name	Description	Data Displayed on Clicking the Links	Applicable Node Types
MySQL	Tables exceed the size limit (<10 GB)	This parameter logs the MySQL database tables that exceed 10 GB.	You are directed to the **Administration > Fabric > Large Database Tables** page. See Table 141 for the details displayed on the page. Click **Close** to return to the Administration statistics page.	Database
Fabric	Audit Logs forwarding failed	This parameter detects and reports the system's failure to forward audit logs to the configured system log server. **NOTE:** On detection and on resolution of an issue, a trap is raised and an e-mail is sent to the Email Listeners list.	You are directed to the **Audit Logs > Audit Log** page with a filtered view of audit logs forwarded to the system log server.	JBoss

Table 136: System Health Report: Processes and Parameters *(continued)*

Process Name	Parameter Name	Description	Data Displayed on Clicking the Links	Applicable Node Types
JBoss	HPROF availability	This parameter detects and logs the Heap and CPU Profiling Agent (HPROF) files on a Junos Space node. The HPROF files are logged in the **/var/cache/jboss** folder on every node.		JBoss

Table 136: System Health Report: Processes and Parameters *(continued)*

Process Name	Parameter Name	Description	Data Displayed on Clicking the Links	Applicable Node Types
			You are directed to the **Administration > Fabric > List of HPROF Files** page with a list of HPROF files. See Table 139 for the details displayed on the page. Click **Close** to return to the Administration statistics page. **NOTE:** • To download HPROF files, select the check boxes corresponding to the HPROF files on the List of HPROF Files page and click the Download icon (top-left corner of the page). The HPROF files are downloaded to the local computer. • To delete selected HPROF files from the List of HPROF Files page, select the check boxes corresponding to the HPROF files and click the Delete icon (top-left corner of the page). The HPROF files are deleted from the List of HPROF Files page. • To delete all HPROF files from the List of HPROF Files page and start monitoring the HPROF file status, select the check boxes corresponding to all the HPROF files and click the Delete icon (top-left corner of the page). The Status column displays a	

Table 136: System Health Report: Processes and Parameters *(continued)*

Process Name	Parameter Name	Description	Data Displayed on Clicking the Links	Applicable Node Types
			green No.	

> **NOTE:** The **VIP Bind issue detected in DB nodes(s), VIP Bind issue detected in FMPM nodes(s), Fabric node in the DOWN state detected, JGroups membership issue detected**, and **Audit Logs forwarding failed** parameters are available from Junos Space Network Management Platform Release 16.1R1 onward.

Table 137: Extended Periods of High CPU Page

Field	Description
Node Name	Logical name assigned to the node
Management IP (IPv4)	IPv4 address for the node
Management IP (IPv6)	IPv6 address for the node
From Time	Time from when the node reported high CPU usage
To Time	Time until when the node reported high CPU usage
Duration (Mins)	Total duration of high CPU usage on the node in minutes
Average CPU (%)	Average load on the CPU of the node

Table 138: Device Management Sessions Page

Field	Description
Host	Name of the host machine and the Junos Space node where the Junos Space Virtual Appliance is deployed
Management IP (IPv4)	IPv4 address for the node
Management IP (IPv6)	IPv6 address for the node

Table 138: Device Management Sessions Page *(continued)*

Field	Description
Time	Time when the count of device management SSH sessions with devices was last calculated
Status	Connection status of the node
Console Count	Number of device management SSH sessions as per the Junos Space database
Number of Devices	Number of devices managed by the Junos Space node

Table 139: List of HPROF Files Page

Field	Description
Node Name	Logical name assigned to the node
Management IP (IPv4)	IPv4 address for the node
Management IP (IPv6)	IPv6 address for the node
File Created Time	Time when the HPROF file was created on the node
File Location	Location of the HPROF file on the node

Table 140: Last JBoss Restarted Time Page

Field	Description
Node Name	Logical name assigned to the node
Management IP (IPv4)	IPv4 address for the node
Management IP (IPv6)	IPv6 address for the node
Last Restart Time	Time when JBoss was last restarted on the node

Table 141: Large Database Tables Page

Field	Description
Database	Type of database: MySQL

Table 141: Large Database Tables Page *(continued)*

Field	Description
Table Name	Name of the table in the database
Time	Time when the size of the database was last updated
Size (GB)	Size of the database in GB

Viewing System Alert Messages in the Last 30 Days

When Junos Space Platform or a Junos Space application tries to contact an active SMTP server (configured on Junos Space) and the connection to the server fails, the System Alert Messages in Last 30 Days box displays the details of SMTP server connection failures. The failures are recorded only for the last 30 days. Table 142 summarizes the information displayed for each failed connection.

Table 142: Details of System Alert Messages

Field	Description
Application	Name of the Junos Space application that tried to contact the SMTP server If Junos Space Platform tried to contact the SMTP server and failed, then **Platform** is displayed.
Category	Displays SMTP for all error messages
Error	Specifies the type of error that occurred
Last Occurrence	Date and time of the last occurrence of the error

Release History Table

Release	Description
16.1R1	
16.1R1	The **VIP Bind issue detected in DB nodes(s), VIP Bind issue detected in FMPM nodes(s), Fabric node in the DOWN state detected, JGroups membership issue detected**, and **Audit Logs forwarding failed** parameters are available from Junos Space Network Management Platform Release 16.1R1 onward.
15.2R1	Starting with Junos Space Network Management Platform Release 15.2R1, you can view records about the health and performance of the Junos Space nodes in your Junos Space setup and the processes on these nodes in a system health report.

RELATED DOCUMENTATION

- Overall System Condition and Fabric Load History Overview | **1159**
- Modifying Junos Space Network Management Platform Settings | **1346**
- Managing SMTP Servers | **1477**

Junos Space IPv6 Support Overview

Starting from Junos Space Network Management Platform Release 14.1R2, you can discover and manage devices by using IPv6 addresses. Junos Space Platform supports the management of devices configured with only IPv4 addresses, only IPv6 addresses, or both. In addition, Junos Space Platform receives traps for IPv6 devices by using IPv6 addresses.

You can also configure IPv6 addresses for the following IP addresses:

- Virtual IP (VIP) address of the Junos Space fabric
- Node management and device management IP addresses of Junos Space nodes
- Administrative interface (eth1) for Junos Space nodes
- Default gateway IP address for Junos Space nodes
- VIP address of the Fault Monitoring and Performance Monitoring (FMPM) nodes
- Node management IP address of FMPM nodes
- Default gateway IP address for Junos Space and FMPM nodes

> **NOTE:** If you configure IPv6 addresses for any of the preceding IP addresses, you must also configure an IPv4 address. Junos Space Platform does not allow you to configure *only* IPv6 addresses for Ethernet interfaces of fabric nodes. Table 143 displays the IP address configurations supported on Junos Space Platform.

Table 143: IP Address Configurations Supported on Junos Space Platform

Type of Addressing Scheme	eth0	VIP	eth1 (Optional)	eth3 (Optional)
IPv4 only (Pure IPv4)	IPv4	IPv4	IPv4	Not configured
	IPv4	IPv4	IPv4	IPv4
	IPv4	IPv4	IPv4	IPv6
IPv4 and IPv6 (Dual Stack)	IPv4	IPv4	IPv4	IPv4 and IPv6
	IPv4 and IPv6	IPv4 and IPv6	IPv4 and IPv6	IPv4 and IPv6

Devices managed by Junos Space Platform can initiate connections by using an IPv4 or IPv6 address. When Junos Space Platform initiates the connection to a device, the type of connection (IPv4 or IPv6) depends on the type of IP address specified during device discovery.

NOTE: For non-SRX Series devices, device-initiated connections to Junos Space Platform that use IPv6 addresses are supported only on Junos OS Release 15.1 or later; this is because IPv6 addresses are supported in the outbound-SSH configuration only from Junos OS Release 15.1 onward for non-SRX Series devices. For SRX Series devices, device-initiated connections to Junos Space Platform that use IPv6 addresses are supported from Junos OS Release 12.1x47D15 onward.

You can also modify the target IP address of a device (from IPv4 to IPv6, IPv4 to IPv4, IPv6 to IPv4, and IPv6 to IPv6), which Junos Space Platform uses to connect to a device. For more information, see "Modifying the Target IP Address of a Device" on page 453.

NOTE: The following limitations are applicable when you use IPv6 addresses:

- IPv6 support for devices depends on the version of Junos OS running on the device; earlier versions of Junos OS might not support IPv6 configuration. IPv6 support for device-initiated connections is available from Junos OS Release 15.1R1 onward.
- All nodes in the Junos Space fabric must have the same type of IP address (or addresses) configured. For example, if a Junos Space node or an FMPM node in a fabric is configured with both IPv4 and IPv6 addresses, then all other Junos Space and FMPM nodes in the fabric must be configured with both IPv4 and IPv6 addresses.

RELATED DOCUMENTATION

Modifying the Target IP Address of a Device | 453

Modifying the Network Settings of a Node in the Junos Space Fabric | 1264

Device Management Overview | 189

Maintenance Mode Overview

In Junos Space Network Management Platform, *maintenance mode* is a special mode that the administrator uses to perform database restore or debugging tasks while all nodes in the fabric are shut down and the Junos Space Platform Web proxy is running.

The Junos Space system goes into maintenance mode in the following cases:

- Junos Space Platform goes down.

  The system goes into maintenance mode when Junos Space Platform is down on all nodes in the fabric. Users attempting to log in when the system is in maintenance mode are redirected to the maintenance mode login page. Users who logged in to Junos Space Platform before the shutdown and attempt to perform an action on the user interface are also redirected to the maintenance mode login page.

- An authorized Junos Space administrator initiates a restore operation from the Database Backup and Restore workspace to restore a database.

  When a user initiates a restore operation, Junos Space Platform prompts the user to type a username and password to enter maintenance mode. After the user is authenticated, Junos Space Platform initiates the restore operation and the system remains in maintenance mode until the database is restored and the user exits maintenance mode.

- An authorized Junos Space administrator upgrades the Junos Space Platform software.

  When a user initiates a software upgrade, Junos Space Platform prompts the user to type a username and password to enter maintenance mode. After the user is authenticated, Junos Space Platform initiates the software upgrade and the system remains in maintenance mode until the upgrade is finished and the user exits maintenance mode.

When a user is authenticated to access Junos Space Platform in maintenance mode, the Maintenance Mode Options page displays the tasks that a user can perform in maintenance mode.

When a user exits maintenance mode, Junos Space Platform is restarted. After several minutes, the system returns to normal operational mode, and Junos Space users can log in to the user interface.

> **NOTE:** During startup, the startup page first displays a message indicating that Junos Space Platform is starting up and then displays a progress bar indicating the percentage of startup completed, the estimated time left for the Junos Space Platform to start, and a list of tasks to complete (with an indication of the current task being carried out). When a task is successfully completed, a message is displayed; if a task fails, an error message is displayed indicating why the task failed.

Maintenance Mode Access and System Locking

An authorized Junos Space administrator puts the system into maintenance mode by initiating a Restore operation.

Only one maintenance-mode administrator can access maintenance mode at a time. When an administrator logs in to maintenance mode, Junos Space Platform locks the page. When a second administrator attempts to log in to maintenance mode while the first administrator is logged in, Junos Space Platform displays a message indicating that another administrator is currently logged in to the system and that maintenance

mode is locked. The maintenance mode lock is released when the first administrator logs out or the lock times out. If the logged-in administrator is inactive, the maintenance mode lock is released after five minutes during which another administrator can log in.

Maintenance-Mode User Administration

The username for the maintenance-mode administrator is 'maintenance'.

You can set the password for the maintenance-mode administrator through the Junos Space system console during the initial installation and configuration of a Junos Space Appliance or Junos Space Virtual Appliance.

A Junos Space administrator connects to a Junos Space Appliance that is already in maintenance mode by using the URL https://*ip-address*/maintenance, where *ip-address* is the Web-access IP address of the Junos Space Appliance.

RELATED DOCUMENTATION

Restoring the Junos Space Network Management Platform Database | **1314**

Backing Up the Junos Space Network Management Platform Database | **1308**

Backing Up and Restoring the Database Overview | **1305**

CHAPTER 69

Managing Nodes in the Junos Space Fabric

IN THIS CHAPTER

- Fabric Management Overview | **1157**
- Overall System Condition and Fabric Load History Overview | **1159**
- Junos Space Nodes and FMPM Nodes in the Junos Space Fabric Overview | **1162**
- Dedicated Database Nodes in the Junos Space Fabric Overview | **1169**
- Cassandra Nodes in the Junos Space Fabric Overview | **1172**
- Adding a Node to an Existing Junos Space Fabric | **1176**
- Starting the Cassandra Service on a Junos Space Node | **1185**
- Viewing Nodes in the Fabric | **1186**
- Monitoring Nodes in the Fabric | **1194**
- Viewing Alarms from a Fabric Node | **1254**
- Shutting Down or Rebooting Nodes in the Junos Space Fabric | **1256**
- Disabling the Cassandra Service on a Junos Space Node | **1258**
- Deleting a Node from the Junos Space Fabric | **1259**
- Resetting MySQL Replication | **1262**
- Modifying the Network Settings of a Node in the Junos Space Fabric | **1264**
- Load-Balancing Devices Across Junos Space Nodes | **1271**
- Replacing a Failed Junos Space Node | **1272**
- Generating and Uploading Authentication Keys to Devices | **1272**
- Configuring the ESX or ESXi Server Parameters on a Node in the Junos Space Fabric | **1278**
- Creating a System Snapshot | **1279**
- Deleting a System Snapshot | **1281**
- Restoring the System to a Snapshot | **1282**
- Creating a Unicast Junos Space Cluster | **1284**
- NAT Configuration for Junos Space Network Management Platform Overview | **1288**
- Configuring the NAT IP Addresses and Ports on Junos Space Platform | **1300**
- Modifying the NAT IP Addresses and Ports on Junos Space Platform | **1302**
- Disabling the NAT Configuration on Junos Space Platform | **1303**

Fabric Management Overview

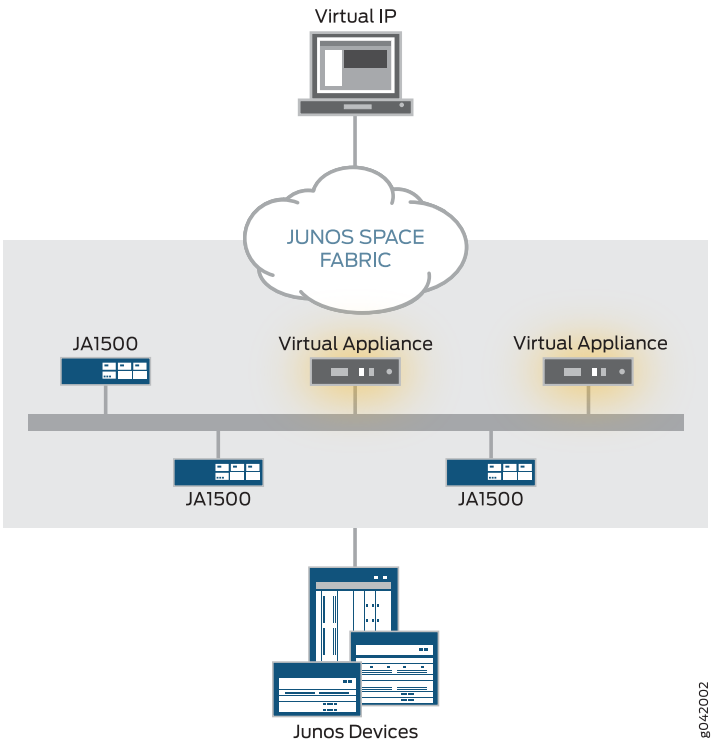
You can deploy a Junos Space Appliance or a Junos Space Virtual Appliance to create a fabric that provides the scalability and availability that your managed network requires as you add more devices, services, and users.

A Junos Space fabric comprises one or more IP-connected nodes. A *node* is a logical object that represents a single Junos Space Appliance (JA1500 or JA2500) or Junos Space Virtual Appliance, its operating system, and the Junos Space Network Management Platform software that runs on the operating system. Each Junos Space Appliance or Junos Space Virtual Appliance that you install and configure is represented as a single node in the fabric. You can add nodes to an existing fabric without disrupting the services that are running on the fabric. For more information about the Junos Space fabric architecture, refer to the *Junos Space Network Management Platform High Availability and Disaster Recovery Guide*.

> **NOTE:** Starting from Release 17.1, Junos Space Platform does not support JA1500 devices.

After you add nodes to the fabric, you can manage and monitor the nodes from the Administration workspace of the Junos Space Platform GUI. To add, manage, and monitor nodes in the fabric, a fabric administrator (that is, a user with the System Administrator privileges) connects to the virtual IP address configured for the fabric, as shown in Figure 49.

Figure 49: Fabric Nodes



NOTE: All nodes that are part of a fabric must have the same version of Junos Space Platform installed.

From the Fabric page of the Administration workspace of the Junos Space Platform GUI, you can perform fabric management tasks, such as adding nodes to the fabric, deleting nodes from the fabric, monitoring nodes, modifying network settings of nodes, rebooting nodes, viewing alarms on a fabric node, load-balancing devices across nodes, generating and uploading authentication keys, creating system snapshots, restoring the system to a system snapshot, and so on.

RELATED DOCUMENTATION

- Junos Space Nodes and FMPM Nodes in the Junos Space Fabric Overview | **1162**
- Viewing Nodes in the Fabric | **1186**
- Adding a Node to an Existing Junos Space Fabric | **1176**
- Monitoring Nodes in the Fabric | **1194**
- Replacing a Failed Junos Space Node | **1272**

Shutting Down or Rebooting Nodes in the Junos Space Fabric | 1256
Viewing Alarms from a Fabric Node | 1254
Load-Balancing Devices Across Junos Space Nodes | 1271
Generating and Uploading Authentication Keys to Devices | 285
Restoring the System to a Snapshot | 1282
Creating a Unicast Junos Space Cluster | 1284

Overall System Condition and Fabric Load History Overview

You can view the overall Junos Space system condition and fabric load from the Junos Space Network Management Platform Dashboard or the Administration statistics page.

Overall System Condition

To calculate the overall Junos Space system condition, Junos Space Platform uses a formula based on cluster health and node-function health:

- Cluster health indicates the percentage of nodes in the fabric that are currently running.

  For example, if only three nodes are reachable in a four-node fabric, cluster health is 75%.

- Load-balancer health indicates the percentage of nodes (enabled for load balancing) that are running the load-balancing process.

  For example, if two nodes are enabled for load balancing and the load-balancing process is running on only one node, the load-balancing health is 50%.

- Database health indicates the percentage of nodes (enabled for database requests) that are running the database process.

  For example, if two nodes are enabled as the database server and the database process is running on only one node, then database health is 50%.

- Application-logic health indicates the percentage of nodes (enabled for application logic (DML and business logic) that are running the application-logic process.

  For example, if three nodes are enabled for application logic and the application-logic process is running on only two nodes, then application-logic health is 67%.

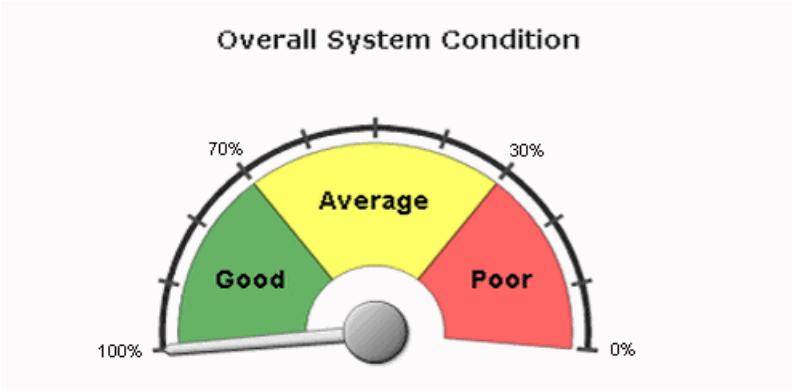
Junos Space Platform retrieves data on the nodes and the node functions that are running, and then applies the following formula to determine the overall Junos Space system condition: Overall System Condition = [(Number of Nodes Running) / (Number of Nodes in Fabric)] * [(Number of Nodes Running Load_Balancing Process) / (Number of Nodes enabled for Load Balancing)] * [(Number of Nodes Running Database-Server

Process) / (Number of Nodes Enabled As Database Server)] * [(Number of Nodes Running Application-Logic Process) / (Number of Nodes Enabled for Application Logic)]

The overall Junos Space system condition is expressed as a percentage. If we use the values in the preceding examples in this formula, then the overall system condition would be calculated as: Overall System Condition = 75% * 50%* 50% * 67% = 12.5%.

A value between 0 and 30% indicates that the system health is Poor, a value between 30% and 70% indicates that the system health is average, and a value between 70% and 100% indicates that the system health is good. The **Overall System Condition** chart displays the system health as shown in Figure 50

Figure 50: Overall System Condition Gauge



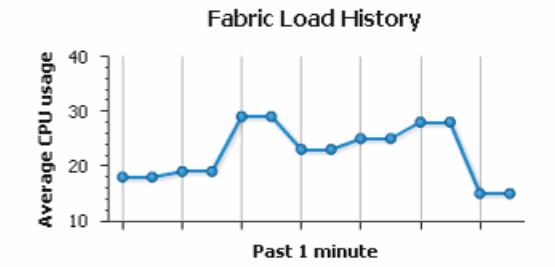
The overall system health indicates 0% (Poor) when any one of the following conditions is detected:

- No nodes in the fabric are running.
- No nodes enabled for load balancing are running the load-balancing process.
- No nodes enabled for database requests are running the database process.
- No nodes enabled for application logic are running the application-logic process.

Fabric Load History

The Fabric Load History chart, as shown in Figure 51, displays the average CPU usage across all nodes that are running in the fabric.

Figure 51: Fabric Load History Chart



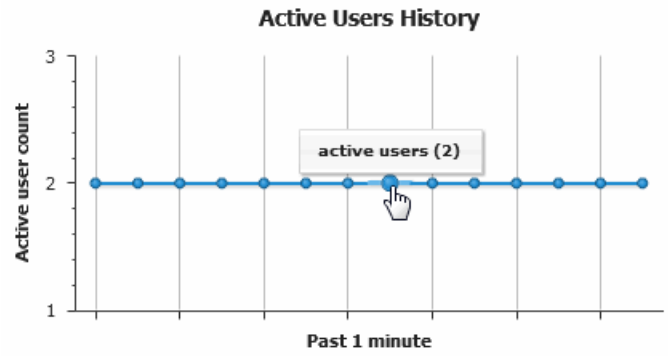
Junos Space Platform uses the following formula to determine the fabric load: Fabric Load = (Total CPU Usage for All Nodes Running) / (Number of Nodes Running)

For example, for a fabric with three nodes running and CPU usage of 80%, 30%, and 10%, respectively, the fabric load is 40%.

Active Users History

The Active Users History chart, as shown in Figure 52, displays the number of active users in the past one minute.

Figure 52: Active Users History Chart



RELATED DOCUMENTATION

- Viewing the Junos Space Platform Dashboard | 126
- Viewing the Administration Statistics | 1138

Junos Space Nodes and FMPM Nodes in the Junos Space Fabric Overview

IN THIS SECTION

- Understanding the Junos Space Node Functions in a Fabric | 1162
- Understanding the FMPM Node Functions in a Fabric | 1166

When you install and configure the Junos Space Appliance or Junos Space Virtual Appliance as a Junos Space node, Junos Space Network Management Platform automatically creates a fabric with one node. To create a fabric with multiple nodes providing the scalability and availability that your network requires, you must first configure a Junos Space Appliance (JA2500) or a Junos Space Virtual Appliance either as a Junos Space node or a dedicated Fault Monitoring and Performance Monitoring (FMPM) node by using the Junos Space CLI. You can then use the Junos Space Platform GUI to add the node to the fabric.

This topic contains the following sections:

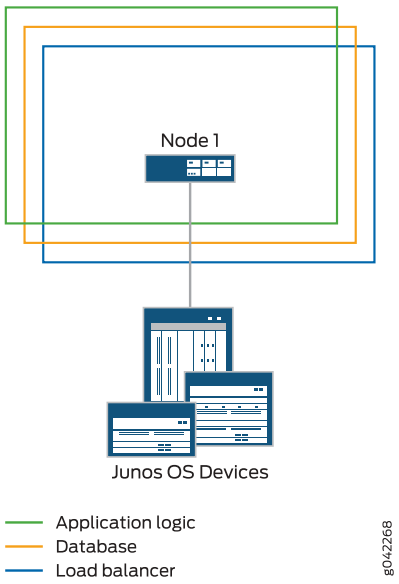
Understanding the Junos Space Node Functions in a Fabric

A fabric that consists of a single node provides complete Junos Space Platform management functionality, with the following node functions enabled for the node:

- Load balancer—For processing HTTP requests from remote browsers and northbound interface (NBI) clients
- Database—For processing database requests (for create, read, update, and delete operations)
- Application logic (JBoss server)—For processing back-end business logic (Junos Space Network Management Platform service requests) and Device Mediation Layer (DML) workload (that is, any interaction between Junos Space and any device, such as device connectivity, device events, and logging events)

Figure 53 shows all functions enabled on a fabric comprising one node.

Figure 53: Fabric with One Node



NOTE: A fabric that comprises a single node provides no workload balancing and no backup if the Junos Space node goes down.

As your network expands with new devices, services, and users, you can add Junos Space nodes to handle the increased workload. For each additional Junos Space node that you configure, you must add the node to the fabric using the Junos Space Platform GUI. Each node that you add to the fabric increases the resource pool for the node functions to meet the scalability and high availability requirements of your network.

The Junos Space Platform node functions distribute the workload across operating nodes according to the following load-distribution rules:

- Load balancer—When a node that functions as the active load-balancer server is down, all HTTP requests are automatically routed to the standby load-balancer server that is running on a separate node.
- Database—When a node that functions as the active database server is down, all database requests (for create, read, update, and delete operations) are routed to the node that functions as the standby database server.
- Application logic (DML and business logic)—Device connections and user requests are distributed among the nodes, and device-related operations are routed to the node to which the device is connected.

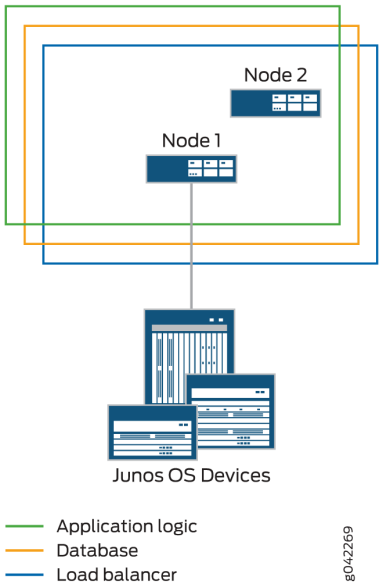
  Junos Space Platform uses the following algorithm to ensure that the number of devices connected to a node does not exceed the threshold limit for each node:

  Threshold Limit = [(Number of Devices in Database) / (Number of Nodes Running)] + 2

When a second Junos Space node is added to the fabric, the first node functions as the active load-balancer server and active database server, and the second node functions as the standby load-balancer server and standby database server. The load-balancer and application logic node functions provide scalability and high availability. The database node function on the second node provides high availability only.

Figure 54 shows the functions enabled on a fabric comprising two nodes.

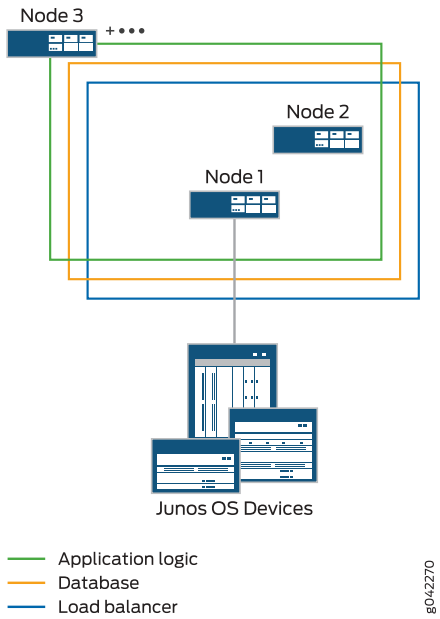
Figure 54: Fabric with Two Nodes



Typically, if the fabric has three or more Junos Space Nodes, only the application logic functionality is enabled from the third node onward. The application logic functionality provides both scalability and high availability. However, high availability for application logic is not available if both the first and second nodes are down. For high availability of application logic, at least one among the first and second nodes should be up.

Figure 55 shows the functions enabled on a fabric comprising three nodes.

Figure 55: Fabric with Three Nodes



In addition to the load balancer and JBoss nodes, you can also include dedicated database nodes and Cassandra nodes in the Junos Space fabric. For more information about dedicated database nodes and Cassandra nodes, see "Dedicated Database Nodes in the Junos Space Fabric Overview" on page 1169 and "Cassandra Nodes in the Junos Space Fabric Overview" on page 1172 respectively.

You can add a Junos Space node to an existing fabric as one of the following types of nodes on the basis of the functions you want the node to perform.

- JBoss, database and load-balancer node:

  When you add a node to an existing fabric that has one JBoss, database and load-balancer node, you can choose to add the new node as another JBoss, database and load-balancer node. This node functions as the standby load-balancer server and ensures high availability for the Junos Space fabric. The node also provides database and application logic functionality to the fabric.

- JBoss and load-balancer node:

  When you add a node to an existing fabric that has two dedicated database nodes in addition to a JBoss and load-balancer node, the fourth node can be added only as another JBoss and load-balancer node. This node functions as the standby load-balancer server and ensures high availability for the Junos Space fabric. In this case, both the active and standby load-balancer nodes provide load balancing and application logic functionality only and the dedicated database nodes provide the database functionality.

- JBoss node:

  When you add a node to an existing fabric that already has two load-balancer nodes, you can choose to add the new node as a JBoss-only node. This node provides only the application logic functionality.

After you add the JBoss node to the fabric, you can choose to enable the Apache Cassandra service on the node to convert the node to a JBoss and Cassandra node.

- Dedicated database node:

  When you add a node to an existing fabric, you can choose to add the node as a dedicated database node. If no dedicated database nodes exist in the fabric, you must add two nodes together, one as the primary database node and the other as the secondary database node. If a dedicated database node is already part of the fabric, you can add one node as the secondary database node. You cannot have more than two dedicated database nodes in a fabric. The dedicated database nodes function as the primary and secondary MySQL servers.

- Dedicated Cassandra node:

  When you add a node to an existing fabric, you can choose to add the node as a dedicated Cassandra node. Dedicated Cassandra nodes run only the Apache Cassandra service. You can have dedicated Cassandra nodes or JBoss nodes that have the Apache Cassandra service running on them as part of a fabric. Both these nodes are referred to as Cassandra nodes in Junos Space Platform and multiple Cassandra nodes together form the Cassandra cluster. The Cassandra nodes in a fabric provide a distributed file system to store device image files in Junos Space Platform.

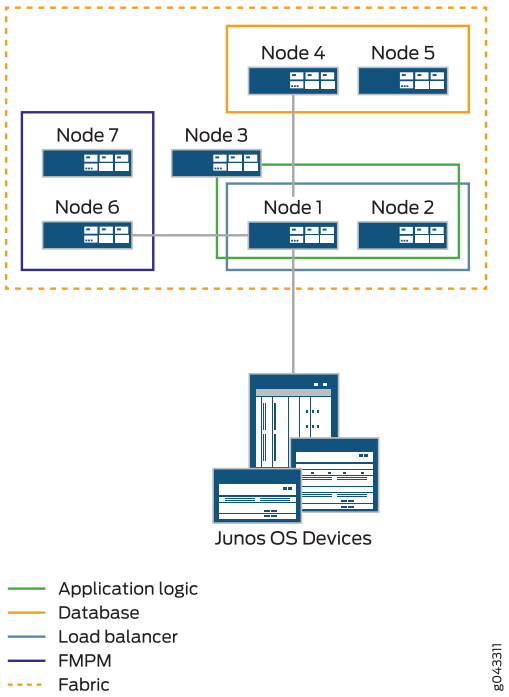
Understanding the FMPM Node Functions in a Fabric

Junos Space nodes have network monitoring (fault monitoring and performance monitoring) capabilities enabled by default. For improved performance, you can configure a dedicated Fault Monitoring and Performance Monitoring (FMPM) node that is used exclusively for network monitoring.

After configuring an FMPM node, you must add the FMPM node to an existing Junos Space fabric for Junos Space Platform and other Junos Space applications to use the services provided by this node. The FMPM nodes that are added to the fabric are deployed into a Junos Space cluster in a fashion similar to a Junos Space node.

Figure 56 shows FMPM functions enabled in a fabric comprising five Junos Space nodes and two FMPM nodes.

Figure 56: Fabric with FMPM Nodes



When you add the FMPM node to the fabric, the network monitoring functionality is disabled on the Junos Space nodes and is enabled on the FMPM node. All the devices and nodes now send their traps to the newly added FMPM node. This feature provides you with a high performance network monitoring solution for networks with more than 15,000 small devices or a few devices with thousands of interfaces.

You can have a cluster of FMPM nodes hosting only the network monitoring functionality. An FMPM cluster can consist of a maximum of two FMPM nodes. The network monitoring service present in an FMPM cluster is considered as a part of Junos Space Platform and can be used by one or more applications. Having more than one FMPM node in a cluster provides high availability (HA).

An FMPM team can monitor the nodes that have been added to the Junos Space fabric and also the devices that have been discovered from Junos Space Platform.

NOTE:

- You can add up to a maximum of two FMPM nodes to an FMPM cluster.
- When the first FMPM node is up, the network monitoring functionality is enabled on this node and the network monitoring database (PostgreSQL database) runs on this node.
- When you add a second FMPM node to the fabric, the first node functions as the primary node, and the second node functions as the standby. The PostgreSQL database is continuously replicated from the primary FMPM node to the secondary FMPM node. However, the configuration files that are stored outside of the PostgreSQL database are backed up only at midnight.
- If the primary FMPM node (first node) is rebooted or if the node is down, the secondary FMPM node automatically takes over the network monitoring functions.

Each node that you add to the fabric increases the resource pool for the node functions to meet the scalability and availability requirements of your network.

After an FMPM node is added to the fabric, you can perform most of the actions that are permitted for a Junos Space node, such as monitoring the FMPM node, modifying the network settings of the node, deleting a node and so on.

RELATED DOCUMENTATION

Fabric Management Overview | **1157**

Adding a Node to an Existing Junos Space Fabric | **1176**

Dedicated Database Nodes in the Junos Space Fabric Overview | **1169**

Cassandra Nodes in the Junos Space Fabric Overview | **1172**

Viewing Nodes in the Fabric | **1186**

Monitoring Nodes in the Fabric | **1194**

Creating a Unicast Junos Space Cluster | **1284**

Dedicated Database Nodes in the Junos Space Fabric Overview

Junos Space Network Management Platform enables the load balancer, application logic, and database functions on the first node of the fabric by default. For improved performance of Junos Space Platform and Junos Space applications, you can add two additional Junos Space nodes to run as dedicated database nodes. You can add any two Junos Space nodes as the primary and secondary database nodes. Database high availability (HA) is enabled by default.

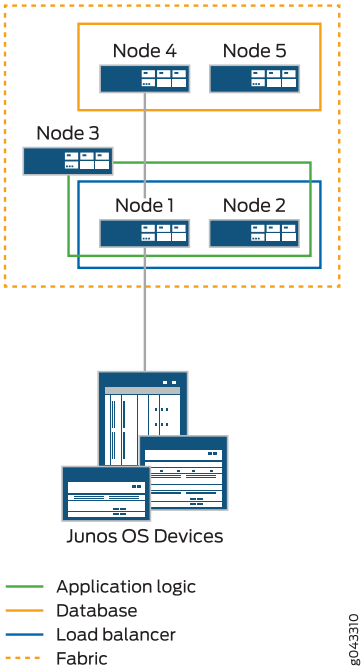
Before you add database nodes to the fabric, you must configure a Junos Space Appliance (JA2500) or a Junos Space Virtual Appliance as a Junos Space node to be added to an existing fabric, by using the Junos Space CLI. You can then use the Junos Space Platform UI to add the node as a dedicated database node to the fabric.

When you add database nodes to the Junos Space fabric, the MySQL database is moved to the primary and secondary database nodes and disabled on the Junos Space active and standby nodes, improving the performance of the Junos Space active node.

Junos Space accesses the database through a database VIP address, which is assigned to the primary database node. You specify the database VIP address when you add the database nodes to the fabric. After you add the database nodes to the Junos Space fabric, Junos Space Platform automatically reconfigures the Junos Space server to use the new database VIP address to access the database

Figure 57 shows database nodes in a fabric comprising five nodes.

Figure 57: Fabric with Database Nodes



In case the primary database node goes down or is deleted, the database VIP address is transferred to the secondary node, which becomes the new primary database node, and any other non-load-balancer node in the fabric can be designated the new secondary database node. If the secondary database node goes down or is deleted, the primary database node retains the database VIP address and you can designate any other non-load-balancer node as the new secondary database node. If there is no other non-load-balancer node in the fabric or you choose not to configure a new secondary database node, database high availability is lost.

When you add database nodes to the fabric, node functions are assigned based on the number and type of nodes that already exist in the fabric.

- Adding database nodes to a fabric with one node—By default, the load-balancer, database server, and application logic node functions are enabled on the first node of the fabric. When you add database nodes to a one-node fabric, you must add the second and third nodes together as dedicated database nodes. The database server functions are moved to the dedicated database nodes from the first node, and the first node no longer provides the database server functions.

  When you have one node of the fabric functioning as the active load-balancer server, and two nodes functioning as the primary and secondary database nodes, the fourth node that you add to the fabric automatically assumes the functions of the standby load-balancer server. All subsequent nodes can have only the application logic, only the Apache Cassandra service, or both enabled.

- Adding database nodes to a fabric with two nodes—When you have two nodes in a fabric, the first node functions as the active load-balancer server and active database server, and the second node functions

as the standby load-balancer server and standby database server. You can add the third and fourth nodes as database nodes. The database server functions are moved to the primary and secondary database nodes and disabled on the first and second nodes.

In this case, after you add the two nodes as database nodes, all additional nodes that you add can have only the application logic, only the Cassandra service, or both enabled.

- Adding database nodes to a fabric with more than two nodes—When you have more than two nodes in a fabric, the first node functions as the active load-balancer server and active database server, and the second node functions as the standby load-balancer server and standby database server. The rest of the nodes can have only the application logic, only the Cassandra service, or both enabled on them. You can add two other nodes as database nodes. The database server functions are moved to the primary and secondary database nodes and disabled on the first and second nodes.

While adding database nodes, you must consider the following points:

- To add a node as a database node, the node must have enough disk space for the MySQL database, and an additional 100 GB of free disk space.
- In the first instance of adding database nodes to the Junos Space fabric, you must configure both the primary and secondary database nodes. You cannot add a primary database node alone. Database high availability is enabled by default.
- If you have already added the primary and secondary database nodes, you cannot add another database node.
- When you configure the primary and secondary database nodes, you must ensure that both the nodes have similar configuration. That is, if one node is a Junos Space Virtual Appliance, then the other node must also be a Junos Space Virtual Appliance with the same configuration for CPU, memory, disk space and so on. Similarly, if one node is a JA2500 Junos Space Appliance, the other node must also be a JA2500 Junos Space Appliance with similar configuration.
- Junos Space Platform does not permit you to delete both the primary and secondary database nodes at the same time. You can delete either the primary database node or the secondary database node, but not both nodes.
- After the MySQL database is moved to the dedicated database nodes, you cannot move it back to the Junos Space active and standby nodes.

RELATED DOCUMENTATION

Junos Space Nodes and FMPM Nodes in the Junos Space Fabric Overview | **1162**

Cassandra Nodes in the Junos Space Fabric Overview | **1172**

Adding a Node to an Existing Junos Space Fabric | **1176**

Viewing Nodes in the Fabric | **1186**

Monitoring Nodes in the Fabric | 1194

Cassandra Nodes in the Junos Space Fabric Overview

The Apache Cassandra service is implemented in Junos Space Network Management Platform Release 15.2R1 to provide a distributed file system to store device image files. Junos Space nodes that have the Cassandra service enabled and running are called Cassandra nodes and when two or more Cassandra nodes exist in a Junos Space fabric, they form the Cassandra cluster. A Cassandra cluster in Junos Space can have nodes running only the Cassandra service (dedicated Cassandra nodes) or JBoss nodes running the Cassandra service, or a combination of both. With the Cassandra service implemented, the device image files are moved from the MySQL database to the Cassandra cluster, thereby improving the performance of the MySQL database.

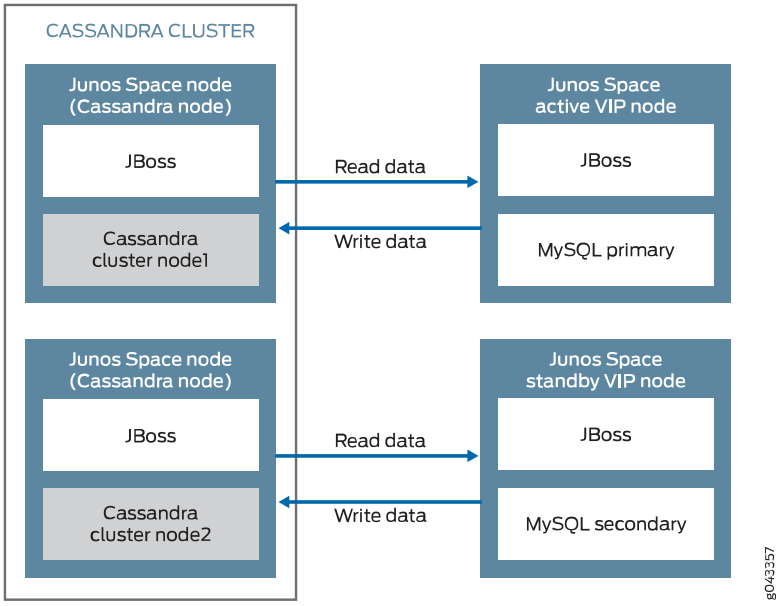
In the Junos Space fabric, Cassandra clusters can have the following types of nodes:

- JBoss nodes with the Cassandra service enabled

  A Cassandra cluster can be formed in a Junos Space fabric by enabling the Cassandra service on JBoss nodes existing in the fabric. When the Cassandra service is enabled on a JBoss node, the node acts as both a JBoss node and Cassandra node.

  Figure 58 shows a Cassandra cluster with the Cassandra service enabled on the existing JBoss nodes.

Figure 58: Cassandra Service on JBoss Nodes



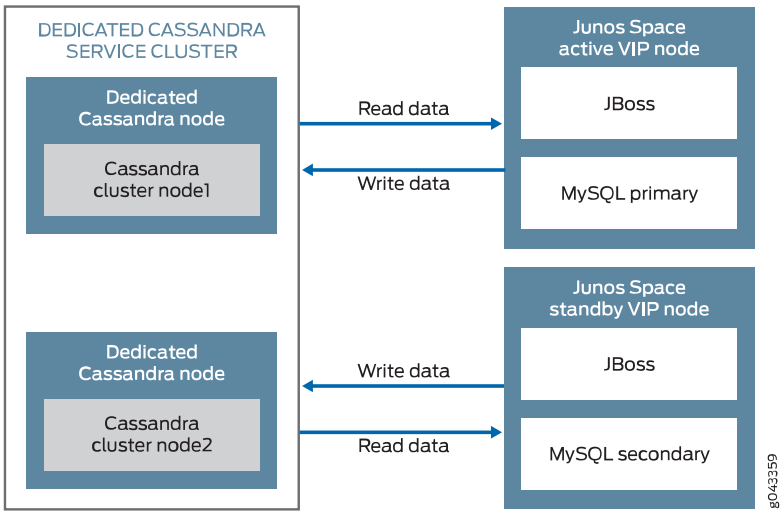
- Dedicated Cassandra nodes

A dedicated Cassandra node provides only the Cassandra service in a fabric. If a dedicated Cassandra node already exists in the fabric, any new dedicated Cassandra node added to the fabric, together with the existing Cassandra node, forms a Cassandra cluster.

Within a fabric, a Cassandra cluster can have any number of Cassandra nodes (that is, a fabric can contain a Cassandra cluster of up to eight Cassandra nodes).

Figure 59 shows a Cassandra cluster with dedicated Cassandra nodes.

Figure 59: Cassandra Service on Dedicated Cassandra Nodes

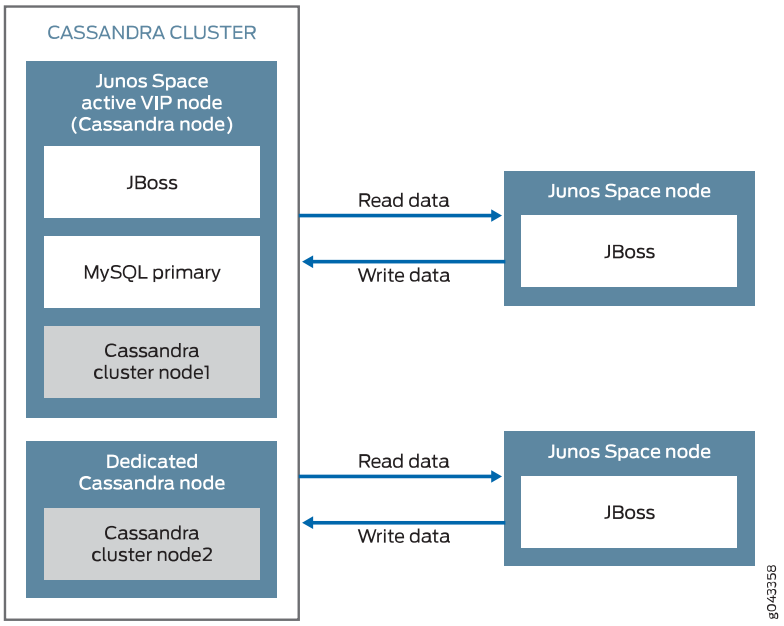


- Dedicated Cassandra nodes and JBoss nodes with the Cassandra service enabled

  A Cassandra cluster can comprise both dedicated Cassandra nodes and JBoss nodes on which the Cassandra service is enabled.

  Figure 60 shows a Cassandra cluster with a JBoss and Cassandra node and a dedicated Cassandra node.

Figure 60: Cassandra Service on JBoss and Dedicated Cassandra Nodes



For a JBoss node to provide the distributed file functionality, you must first enable and then start the Cassandra service. You can enable, disable, start, or stop the Cassandra service on a JBoss node from the Junos Space Platform GUI.

NOTE: You cannot start the Cassandra service on dedicated database nodes or Fault Monitoring and Performance Monitoring (FMPM) nodes.

You can also use the command-line interface of a JBoss node to monitor the Cassandra cluster in a fabric as follows:

- To monitor the Cassandra cluster, use the **nodetool status** command.

  The **nodetool** utility lists all the nodes in the Cassandra cluster and their status as shown in the following sample:

```
[user@host ~]# nodetool status platform
Datacenter: DC1
===============
Status=Up/Down
|/ State=Normal/Leaving/Joining/Moving
--  Address       Load       Tokens  Owns (effective)  Host ID
              Rack
UN  192.0.2.120  75.39 KB   256     100.0%
```

```
844cf4c4-e6ad-498a-a85f-c841d1f72419  RAC1
UN  192.0.2.121  84.94 KB   256     100.0%
d670b1b8-d2a4-41b0-badb-0fc61dc88a5c  RAC1
```

- The Cassandra service provides the cqlsh command-line tool for interacting with the Cassandra database.

  You can connect to the Cassandra database from any JBoss node by using the **cqlsh *<ip address>* -u *<username>* -p *<password>*** command, where *<ip address>* is the IP address of the Cassandra node, *<username>* is the username and *<password>* is the password used to access the Cassandra node.

```
[user@host]# cqlsh 192.0.2.120 -u test-user -p test-pwd
Connected to Test Cluster at 192.0.2.120:9042
[cqlsh 5.0.1 | Cassandra 2.1.2 | CQL spec 3.2.0 | Native protocol V3]
Use HELP for help

cqlsh>
```

Release History Table

Release	Description
15.2R1	The Apache Cassandra service is implemented in Junos Space Network Management Platform Release 15.2R1 to provide a distributed file system to store device image files.

RELATED DOCUMENTATION

- Junos Space Nodes and FMPM Nodes in the Junos Space Fabric Overview | **1162**
- Adding a Node to an Existing Junos Space Fabric | **1176**
- Starting the Cassandra Service on a Junos Space Node | **1185**
- Disabling the Cassandra Service on a Junos Space Node | **1258**
- Fabric Management Overview | **1157**

Adding a Node to an Existing Junos Space Fabric

IN THIS SECTION

- Adding a Junos Space Node to the Junos Space Fabric | 1177
- Adding an FMPM Node to the Junos Space Fabric | 1182
- Obtaining Fingerprint of a Junos Space Node | 1183

When you configure a JA2500 Junos Space Appliance JA2500) or a Junos Space Virtual Appliance as a Junos Space node by using the Junos Space CLI, Junos Space Network Management Platform automatically adds the first node to the fabric. By default, the Junos Space fabric contains this single node that provides complete Junos Space Platform functionality. For each additional node that you install and configure, you must add the node from the Junos Space Platform UI to represent the node in the fabric.

Before you begin, the following prerequisites must be in place:

- Multicast must be enabled on the switches to which Junos Space nodes are connected.
- IGMP-snooping needs to be disabled on the switches to which Junos Space nodes are connected. By default, IGMP-snooping is enabled on most switches.
- All Junos Space nodes must be interconnected using a high-speed (1-Gbps or 100-Mbps) network with a maximum latency not exceeding 300 milliseconds.

Using the Junos Space CLI, you can configure a Junos Space Appliance or a Junos Space Virtual Appliance either as a Junos Space node or a Fault Monitoring and Performance Monitoring (FMPM) node. If you want to add a node to the fabric as a dedicated database node or a dedicated Cassandra node, it must be configured as a Junos Space node.

For information about how to configure a Junos Space Virtual Appliance as a Junos Space node, see *Configuring a Junos Space Virtual Appliance as a Junos Space Node* in the *Junos Space Virtual Appliance Installation and Configuration Guide* and for information about how to configure a JA2500 appliance as a Junos Space node, see *Configuring a Junos Space Appliance as a Junos Space Node* in the *JA2500 Junos Space Appliance Hardware Guide*.

For information about how to configure a Junos Space Virtual Appliance as an FMPM node, see *Configuring a Junos Space Virtual Appliance as a Standalone or Primary FMPM Node* or *Configuring a Junos Space Virtual Appliance as a Backup or Secondary FMPM Node for High Availability* in the *Junos Space Virtual Appliance Installation and Configuration Guide*. For information about how to configure a JA2500 appliance as an FMPM node, see *Configuring a Junos Space Appliance as a Standalone or Primary FMPM Node* or *Configuring a Junos Space Appliance as a Backup or Secondary FMPM Node for High Availability* in the *JA2500 Junos Space Appliance Hardware Guide*.

NOTE: If you want to change an existing Junos Space node to an FMPM node or vice versa, you must reimage the appliance and reconfigure it as an FMPM node or a Junos Space node. For more information, refer to the Junos Space Appliance and Junos Space Virtual Appliance documentation.

NOTE:
Before you add a node to the Junos Space fabric, verify the following:

- The version of Junos Space Platform installed on the node is the same as the version installed on other nodes in the fabric.
- Ensure that no jobs are pending.
- If a Junos Space node, a database node, or an FMPM node that is part of an existing fabric is deleted, then you need to reimage the node before the node can be readded to the fabric. Junos Space displays the following message when you try to add such nodes to an existing fabric:
  The node you are trying to add was part of another fabric, please re-image the node before adding to this fabric.
- Ensure that you are not adding a non-FMPM node as an FMPM node. Junos Space Platform displays the following message when you try to add such a node to the fabric:
  Node agent is not running on {0}. Please make sure the node being added is not a specialized node.

From the Junos Space Platform UI, you can add a node to the Junos Space fabric by executing one of the following procedures, based on whether you have configured the node as a Junos Space node or as an FMPM node.

Adding a Junos Space Node to the Junos Space Fabric

To add a Junos Space node to the fabric:

1. On the Junos Space Platform UI, select **Administration > Fabric**.

   The **Fabric** page appears.

2. Click the **Add Fabric Node** icon.

   The **Add Node to Fabric** page appears.

3. Click the appropriate option button in the **Node Type** field to select the type of node you want to add.

NOTE: The options that are displayed depend on the number and type of nodes that are already part of the fabric.

Table 144 describes the options that you can select while adding Junos Space nodes.

Table 144: Number of Existing Nodes and Permitted Node Types

Number of Nodes Existing in the Fabric	Permitted Node Types	Description
One	**JBoss and DB Node** **DB Node** **Dedicated Cassandra Node**	When you add the second Junos Space node to the default single-node Junos Space fabric, you can add the new node as a JBoss and database node (standby load-balancer server), a dedicated Cassandra node, or the second and third nodes together as database nodes. In the case of database nodes, one node is designated the primary database node, and the other the secondary database node. The database VIP address must also be configured to enable database high availability.
Two	**JBoss Node** **DB Node** **Dedicated Cassandra Node**	When you add nodes to a two-node Junos Space fabric, Junos Space Platform allows you to add a JBoss node, a dedicated Cassandra node, or two nodes as database nodes. In the case of database nodes, one node is designated the primary database node, and the other the secondary database node. The database VIP address must also be configured to enable database high availability. If the Junos Space fabric already has one database node added, then you can add either a JBoss-only node or one database node as the secondary database node. The database node already existing in the fabric is the primary database node.
Three or more—With one or no database node configured	**JBoss Node** **DB Node** **Dedicated Cassandra Node**	When you add nodes to a Junos Space fabric with three or more nodes, with no database nodes added, Junos Space Platform allows you to add a JBoss node, a dedicated Cassandra node, or two nodes as database nodes. If the Junos Space fabric already has one database node added, then you can add a JBoss node, a dedicated Cassandra node, or one database node as the secondary database node. The database node already existing in the fabric is the primary database node.

Table 144: Number of Existing Nodes and Permitted Node Types *(continued)*

Number of Nodes Existing in the Fabric	Permitted Node Types	Description
Three or more—With two database nodes configured	**JBoss Node** **Dedicated Cassandra Node**	When you add nodes to a Junos Space fabric with three or more nodes, with two database nodes already configured, Junos Space Platform allows you to add either a JBoss node or a dedicated Cassandra node. You cannot add more than two database nodes to the fabric.

> **NOTE:** You can enable the Apache Cassandra service on any of the JBoss nodes added to the fabric to convert them to JBoss, Cassandra and database nodes or JBoss and Cassandra nodes. For more information about enabling the Cassandra service, see "Starting the Cassandra Service on a Junos Space Node" on page 1185.

4. Perform one of the following procedures, based on the type of node you selected:

- For the **JBoss and DB Node**, **JBoss Node**, and **Dedicated Cassandra Node** options, perform the following steps:

  a. Enter a name for the node in the **Name** text box.

     The name of the fabric node cannot exceed 32 characters and cannot contain spaces.

  b. Enter the IP address of the node in the **IP address** field.

     This is the IP address for the eth0 interface that you specified during the basic configuration of the appliance.

  c. Enter the username in the **User** field.

  d. Enter the password in the **Password** field.

     > **NOTE:** The login credentials that you specify in the User and Password fields must be the same username and password that you specified for SSH access using the Junos Space CLI during the initial installation and configuration of the node. If the credentials do not match, the node is not added.

  e. (Optional) Enter the fingerprint for the node in the **Fingerprint** field.

> **NOTE:** To obtain the fingerprint of a node, see "Obtaining Fingerprint of a Junos Space Node" on page 1183.

- For the **DB Node** option, perform the following steps:
  - In the **Primary database** section:

    > **NOTE:** If you already have a database node as part of the fabric, the **Primary database** section does not appear. The existing database node is the primary database node and you can add only a secondary database node to the fabric.

    a. Enter a name for the primary database node in the **Name** text box.

       The name of the fabric node cannot exceed 32 characters and cannot contain spaces.

    b. Enter the IP address of the primary database node in the **IP address** field.

       This is the IP address for the eth0 interface that you specified during the basic configuration of the appliance.

    c. Enter the username in the **User** field.

    d. Enter the password in the **Password** field.

       > **NOTE:** The login credentials that you specify in the User and Password fields must be the same username and password that you specified for SSH access using the Junos Space CLI during the initial installation and configuration of the node. If the credentials do not match, the node is not added.

    e. (Optional) Enter the fingerprint for the node in the **Fingerprint** field..

       > **NOTE:** To obtain the fingerprint of a node, see "Obtaining Fingerprint of a Junos Space Node" on page 1183.

    f. Enter the VIP address for the database nodes in the **VIP** field.

The VIP address is used for communication between Junos Space nodes and database nodes. This IP address must be in the same subnet as the IP address assigned to the eth0 Ethernet interface, and the database VIP address must be different from the VIP address used to access the Web GUI and the FMPM nodes.

- In the **Secondary database** section:

  a. Enter a name for the secondary database node in the **Name** text box.

  The name of the fabric node cannot exceed 32 characters and cannot contain spaces.

  b. Enter the IP address of the secondary database node in the **IP address** field.

  This is the IP address for the eth0 interface that you specified during the basic configuration of the appliance.

  c. Enter the username in the **User** field.

  d. Enter the password in the **Password** field.

  > **NOTE:** The login credentials that you specify in the User and Password fields must be the same username and password that you specified for SSH access using the Junos Space CLI during the initial installation and configuration of the node. If the credentials do not match, the node is not added.

  e. (Optional) Enter the fingerprint for the node in the **Fingerprint** field..

  > **NOTE:** To obtain the fingerprint of a node, see "Obtaining Fingerprint of a Junos Space Node" on page 1183.

5. (Optional) Select the **Schedule at a later time** check box to specify a later date and time when you want the node to be added.

   If you do not specify a date and time for adding the node, the node is added to the fabric when you complete this procedure and you click **Add** on the **Add Node to Fabric** page.

   a. Click the calendar icon and select the date.

   b. Click the arrow beside the time list and select the time.

> **NOTE:** The selected time in the scheduler corresponds to the Junos Space server time but is mapped to the local time zone of the client computer.

6. Click **Add** to add the node to the fabric.

   The **Job Information** dialog box appears, with a message indicating that the job to add the node is successfully scheduled. You can click the *job ID* link that is displayed in the dialog box to view job details. You can also navigate to the Job Management page to view job details.

7. Click **OK**.

   You are returned to the **Fabric** page.

   The node is added to the fabric and appears on the **Fabric** page. When you add a node, the node functions are automatically assigned by Junos Space Platform.

Adding an FMPM Node to the Junos Space Fabric

To add an FMPM node to the fabric:

1. On the Junos Space Platform UI, select **Administration > Fabric**.

   The **Fabric** page appears.

2. Click the **Add Fabric Node** icon.

   The **Add Node to Fabric** page appears.

3. Click the **Specialized Node** option button in the **Node Type** field to add an FMPM node.

4. Enter a name for the node in the **Name** text box.

   The name of the fabric node cannot exceed 32 characters and cannot contain spaces.

5. Enter the IP address of the node in the **IP address** field.

   > **NOTE:** This is the IP address for the eth0 interface that you specified during the basic configuration of the appliance.

6. Enter the SSH username for the FMPM node in the **User** field.

7. Enter the password in the **Password** field.

   The login credentials (SSH username and password) of the FMPM node that you specify in the **User** and **Password** fields must be the same username and password that you specified when you initially configured the node from the Junos Space CLI. If the credentials do not matcjh, the node is not added.

8. (Optional) Enter the fingerprint for the node in the **Fingerprint** field.

   > **NOTE:** To obtain the fingerprint of a node, see "Obtaining Fingerprint of a Junos Space Node" on page 1183.

9. (Optional) Select the **Schedule at a later time** check box to specify a later date and time when you want the node to be added.

   If you do not specify a date and time for the node to be added, the node is added to the fabric when you complete this procedure and you click **Add** on the **Add Node to Fabric** page.

   a. Click the calendar icon and select the date.

   b. Click the arrow beside the time list and select the time.

   > **NOTE:** The selected time in the scheduler corresponds to the Junos Space server time but is mapped to the local time zone of the client computer.

10. Click **Add** to add the node to the fabric.

    The **Job Information** dialog box appears, with a message indicating that the job to add the node is successfully scheduled. You can click the *job ID* link that is displayed in the dialog box to view job details. You can also navigate to the Job Management page to view job details.

11. Click **OK**.

    You are returned to the **Fabric** page.

The node is added to the fabric and appears on the **Fabric** page. When you add a node, the node functions are automatically assigned by Junos Space Platform.

Obtaining Fingerprint of a Junos Space Node

In a Junos Space cluster, the fingerprint of a node helps in authenticating and authorizing the node.

Starting from Junos Space Network Management Platform Release 17.1R1, the Fingerprint field is introduced to authenticate and authorize a node before adding the node to a Junos Space cluster.

To obtain the fingerprint of a Junos Space node:

1. Log in to access the command prompt of the node.

   The Junos Space Settings menu appears.

2. Type **6** if the node is a JA2500 appliance or type **7** if the node is a Junos Space Virtual Appliance to access the shell.

   You are prompted to enter the administrator password.

3. Enter the administrator password for the node..

   The shell prompt appears.

4. Enter the **ssh-keygen -lf /etc/ssh/ssh_host_rsa_key -E md5** command as shown below to obtain the fingerprint of the node:

   ```
   [root@space]# ssh-keygen -lf /etc/ssh/ssh_host_rsa_key -E md5
   ```

   The node outputs its fingerprint as shown below:

   ```
   2048 MD5:xx:xx:xx:00:00:00:0x:xx:x0:x0:00:00:x0:xx:00:x0:00
   /etc/ssh/ssh_host_rsa_key.pub (RSA)
   ```

   MD5:xx:xx:xx:00:00:00:0x:xx:x0:x0:00:00:x0:xx:00:x0:00 is the fingerprint in the MD5 format.

   NOTE: Do not include MD5: when you enter fingerprint in the Fingerprint field while adding the node to a cluster.

Release History Table

Release	Description
17.1R1	Starting from Junos Space Network Management Platform Release 17.1R1, the Fingerprint field is introduced to authenticate and authorize a node before adding the node to a Junos Space cluster.

RELATED DOCUMENTATION

Fabric Management Overview | 1157

Viewing Nodes in the Fabric | 1186

Dedicated Database Nodes in the Junos Space Fabric Overview | 1169

Overall System Condition and Fabric Load History Overview | 1159

Cassandra Nodes in the Junos Space Fabric Overview | 1172

Starting the Cassandra Service on a Junos Space Node

You can add Cassandra nodes to a Junos Space fabric by adding nodes that provide only the Apache Cassandra service (known as dedicated Cassandra nodes) or by enabling the Cassandra service on JBoss nodes already present in the fabric.

> **NOTE:** You cannot start the Cassandra service on dedicated database nodes or Fault Monitoring and Performance Monitoring (FMPM) nodes.

For information about adding dedicated Cassandra nodes to a fabric, see "Adding a Node to an Existing Junos Space Fabric" on page 1176.

To enable and start the Cassandra service on a JBoss node:

1. On the Junos Space Platform UI, select **Administration > Fabric**.

   The Fabric page appears.

2. Select a JBoss node on which you want to run the Cassandra service.

3. Select **Actions > Enable Cassandra** to enable the Cassandra service.

   A confirmation dialog box appears.

4. Click **Yes** to enable the Cassandra service on the JBoss node.

   A job is created to enable the Cassandra service on the JBoss node.

5. (Optional) Navigate to the Job Management page to view job details.

6. After the Cassandra service is enabled, on the Fabric page, select the JBoss node on which you want to run the Cassandra service.

7. Click **Start Cassandra** to start the Cassandra service on the JBoss node.

   A confirmation dialog box prompts you to confirm that you want to start the Cassandra service.

   > **NOTE:** Alternatively, you can use the **service cassandra start** command on the node CLI to start the Cassandra service.

8. Click **Yes**.

   The Status dialog box displays the status of the start the Cassandra service operation.

RELATED DOCUMENTATION

Cassandra Nodes in the Junos Space Fabric Overview | 1172

Disabling the Cassandra Service on a Junos Space Node | 1258

Viewing Nodes in the Fabric

IN THIS SECTION

- Changing Views | 1186
- Viewing Fabric Node Details | 1187

The Fabric Monitoring inventory page allows the administrator to monitor each node in the Junos Space fabric. You can also monitor the status of the database, load balancer, and application logic functions running on each node, identify nodes that are overloaded or down, and view when the node was rebooted. The Fabric inventory page refreshes every 10 seconds, by default.

Changing Views

You can display fabric monitoring in tabular view. The fabric nodes appear in a table sorted by node name. Each fabric is a row in the Fabric Monitoring table.

To change views:

1. Select **Administration > Fabric**. The **Fabric** page appears.

2. Click a view indicator at the left of the title bar of the Fabric page.

Viewing Fabric Node Details

To view detailed runtime and status information for a node:

1. On the Junos Space Network Management Platform user interface, select **Administration** > **Fabric**.

   The Fabric page that appears displays all the nodes in the Junos Space Platform fabric.

2. Right-click a node and select **View Fabric Node Details** or double-click inside a row corresponding to a node.

   The **View Node Detail** pop-up window that appears displays three tabs: **Node Detail**, **Reboot Detail**, and **Process Detail**.

3. To view the node details, click the **Node Detail** tab.

   Table 145 describes the details of the node.

   Table 145: Information on the Node Detail Tab

Information	Description
Node name	Logical name assigned to the node **NOTE:** For the first node, Junos Space uses the node name that the user specifies during the initial configuration of the Junos Space Appliance (physical or virtual). For each subsequent node, the user must specify a node name when adding the node to the fabric.
Management IP (IPv4)	IPv4 address for the node
Management IP (IPv6)	IPv6 address for the node
Host Name	Host name of the node
Device Connection IP (IPv4)	IPv4 address for connecting to the device

Table 145: Information on the Node Detail Tab *(continued)*

Information	Description
Device Connection IP (IPv6)	IPv6 address for connecting to the device
Status	Connection status for the node • UP—Node is connected to the fabric • DOWN—Node is disconnected from the fabric
% CPU	Percentage of CPU resource utilized by the node; from 0 to 100% • Unknown—Percentage of CPU utilized is unknown, for example, because the node is not connected
% Memory	Percentage of memory resource utilized by the node; from 0 to 100% • Unknown—Percentage of memory utilized is unknown, for example, because the node is not connected
% SWAP	Percentage of swap memory used • Unknown—Percentage of SWAP memory utilized is unknown, for example, because the node is not connected
% DISK	Percentage of the **/var** directory utilized by the node; from 0 to 100% • Unknown—Percentage of the **/var** directory utilized by the node is unknown, for example, because the node is not connected
App Logic	Application logic function status for the node • UP—Application logic function is running on the node • DOWN—Application logic function enabled on the node but is not running • Unknown—Status for the application logic function is unknown, for example, because the node is not connected • N/A— Application logic function is not configured to run on the node • (Primary)—Configured primary Junos Space node in the fabric • FMPM (Primary)—The configured primary Fault Monitoring and Performance Monitoring (FMPM) node in the fabric • FMPM—The configured secondary FMPM node in the fabric • **Deploying**—Junos Space Platform and its applications are initializing after a recent JBoss restart • **Parsing Schema**—Device schema files are being parsed after a recent JBoss restart

Table 145: Information on the Node Detail Tab *(continued)*

Information	Description
Database	Database function status for the node • UP(Primary)—Database function is running on the node and the node is the primary database node • UP—Database function is running on the node In the case of dedicated database nodes, the secondary database node is always UP. • DOWN—Database function that is enabled on the node but is not running • **Standby**—Database function is on standby and could potentially transition to the UP state on failover • Unknown—Status for the database function is unknown, for example, because the node is not connected • N/A—Database function is not configured to run on the node **NOTE:** By default, the database function is enabled on no more than two nodes in the fabric.
Load balancer	Load balancer function for the node • UP—Load balancer function is running on the node • DOWN—Load balancer function that is enabled on the node is not running • **Standby**—Load balancer function is on standby and could potentially transition to the UP state on failover • Unknown—Status for the Load balancer function is unknown, for example, because the node might not be connected • N/A—Load balancer function is not running because it is not configured to run on the node **NOTE:** By default, the Load balancer function is enabled on no more than two nodes in the fabric. • (VIP)—Configured virtual IP node in the fabric
Hardware model	Model of the Junos Space Appliance **NOTE:** The hardware model, which is applicable only to the hardware appliance, appears when you double-click a table row for a detailed view of the node.
Software version	Junos Space Network Management Platform release version **NOTE:** Software version appears when you double-click a table row for a detailed view of the node.

Table 145: Information on the Node Detail Tab *(continued)*

Information	Description
Serial number	The serial number for the Junos Space Appliance **NOTE:** Serial number appears when you double-click a table row for a detailed view of the node.
Cluster Member IPs	IP addresses of the nodes in the fabric
Is Master Node	Indicates whether the node is a primary node: • TRUE—The node is a primary node • FALSE—The node is not a primary node
Is VIP Node	Indicates whether the node is a virtual IP (VIP) node. The first (active) node and second (standby) node are VIP nodes. • TRUE—The node is a VIP node. • FALSE—The node is not a VIP node.
Virtual Machine(s)	Lists the virtual machine IPs hosted by the node.
Host IP	IP address of the hosted virtual machine. This field is not applicable to Junos Space nodes and Fault Monitoring and Performance Monitoring (FMPM) nodes.

4. To view the details of the last reboot performed, select the **Reboot Detail** tab.

   Table 146 lists the information related to the last reboot performed on this node.

   Table 146: Information on the Reboot Detail Tab

Information	Description
Last Boot Time	Time at which the node was rebooted
Last Boot Reason	Reason why the node was rebooted
Last Rebooted By	Username of the user who rebooted the node

   NOTE: If the node was rebooted from the CLI, or as a result of an upgrade or a fresh installation, the Last Rebooted By column displays **#system**.

   Table 147 lists the default messages displayed to the user for different types of reboot actions.

Table 147: Default Messages for Different Reboot Actions

Reboot Action	Default Message
Rebooting after changing the network settings of the node from the Junos Space user interface	Reboot after Space Network Settings change
Upgrading Junos Space Platform	Space reboot after Software Upgrade
Rebooting from the CLI	Reboot from Shell/Other
Starting up Junos Space Platform for the first time	Junos Space startup after Installation/Software Upgrade

5. To view the details of the processes on this node, select the **Process Detail** tab.

   Table 148 lists the columns that specify the details of the following processes: JBoss, Apache Web Proxy, MySQL, OpenNMS, and PostgreSQL.

   Table 148: Columns on the Process Detail Tab

Column Name	Description
Process	Name of the process
Status	Status of the process: UP, DOWN, STANDBY, or N/A
%CPU	Percentage of CPU resources used by the process on the node
%MEMORY	Percentage of memory used by the process on the node
Start Time	Time at which the process is initiated

   NOTE: The status of the process and the percentage of CPU resources used by the process is queried once every 30 seconds.

   Table 149 lists the different statuses of the following processes: JBoss, Apache Web Proxy, MySQL, OpenNMS, PostgresSQL, and Cassandra.

   Table 149: Process Status

Process Status	Description
UP	The process is up and active.

Table 149: Process Status *(continued)*

Process Status	Description
DOWN	The process is down and inactive.
STANDBY	The process is in standby mode and could potentially transition to the UP state on failover.
N/A	The process is never expected to be active on the node.

> **NOTE:** If the MySQL database replication between nodes is broken, the MySQL process displays the status **OUT OF SYNC**. If the secondary database is in the process of receiving data and the primary database is still executing transactions then the status is **Syncing**. If the MySQL transactions are up-to-date between nodes, the MySQL process displays the status **UP**.

Table 150 describes the behavior and the expected status of the processes when OpenNMS is running on the Junos Space node.

Table 150: Status of the Processes When OpenNMS Is Running on the Junos Space Node

Process	Junos Space Node with OpenNMS		
	VIP Node	Secondary Node	Other Nodes
Apache Web Proxy	UP/DOWN	STANDBY	N/A
JBoss	UP/DOWN	UP/DOWN	UP/DOWN
MySQL	UP/DOWN	UP/DOWN	N/A
OpenNMS	UP/DOWN	STANDBY	N/A
PostgresSQL	UP/DOWN	UP/DOWN	N/A
Cassandra	UP/DOWN	UP/DOWN	UP/DOWN

Table 151 describes the behavior and the expected status of the processes when OpenNMS is running on the FMPM node.

Table 151: Status of the Processes When OpenNMS Is Running on the FMPM Node

Process	Junos Space Node			FMPM Node	
	VIP Node	Secondary Node	Other Nodes	OpenNMS VIP Node	OpenNMS Secondary Node
Apache Web Proxy	UP/DOWN	STANDBY	N/A	N/A	N/A
JBoss	UP/DOWN	UP/DOWN	UP/DOWN	N/A	N/A
MySQL	UP/DOWN	UP/DOWN	N/A	N/A	N/A
OpenNMS	N/A	N/A	N/A	UP/DOWN	STANDBY
PostgresSQL	N/A	N/A	N/A	UP/DOWN	UP/DOWN
Cassandra	UP/DOWN	UP/DOWN	UP/DOWN	N/A	N/A

NOTE: If an unexpected process is running on a node, the status of the process is shown as UP. If a node fails, the status of all processes on the node is shown as UNKNOWN.

For more information about modifying data on the Fabric inventory page, see "Junos Space User Interface Overview" on page 89.

RELATED DOCUMENTATION

- Overall System Condition and Fabric Load History Overview | **1159**
- Fabric Management Overview | **1157**
- Monitoring Nodes in the Fabric | **1194**
- Load-Balancing Devices Across Junos Space Nodes | **1271**
- Modifying the Network Settings of a Node in the Junos Space Fabric | **1264**

Monitoring Nodes in the Fabric

IN THIS SECTION

- Viewing and Modifying the SNMP Configuration for a Fabric Node | **1194**
- Starting SNMP Monitoring on Fabric Nodes | **1248**
- Stopping SNMP Monitoring on Fabric Nodes | **1249**
- Restarting SNMP Monitoring on Fabric Nodes | **1250**
- Adding a Third-Party SNMP V1 or V2c Manager on a Fabric Node | **1250**
- Adding a Third-Party SNMP V3 Manager on a Fabric Node | **1251**
- Deleting a Third-Party SNMP Manager from a Fabric Node | **1253**
- Installing StorMan RPM for Monitor RAID Functionality | **1253**

As an administrator or operator, you can use Junos Space to track the status of physical and logical components of deployed nodes in a fabric.

Junos Space Network Management Platform supports SNMP Monitoring by an SNMP Manager for SNMP v1, v2c, and v3.

The SNMP manager polls Junos Space to obtain information about the logical components of the nodes using an object identifier (OID) in SNMP v1 and v2, or v3 as a user. The response is provided by the Junos Space SNMP agent and the polled data is displayed in the Network Monitoring workspace.

This topic contains the following sections:

Viewing and Modifying the SNMP Configuration for a Fabric Node

To view and edit the Junos Space SNMP configuration for self-monitoring:

1. Select **Administration** > **Fabric**.

   The Fabric page appears.

2. Select the node whose configuration you want to view or modify, and from the Actions menu, select **SNMP Configuration**.

   The SNMP Configuration window appears with the title bar displaying the IP address of the selected node.

3. Set the SNMP configuration parameters as required, using Table 152 to guide you.

NOTE: By default, the system load parameters are set to 4, which means that an alert is indicated only when all CPUs are under 100 percent load.

Table 152: SNMP Configuration

Setting	Explanation	Recommended Settings	Default Value
Enable SNMP over TCP	Enables SNMP communication over TCP **NOTE:** By default, SNMP communication occurs over UDP.	Cleared	Cleared
Monitor Web Service	Includes monitoring the performance of the Junos Space GUI **NOTE:** This parameter is enabled only for the Junos Space VIP node.	Selected	Selected
Monitor All Disks	Includes all disks on the current Junos Space server	Cleared	Cleared
Monitor RAID	Enables Net-SNMP to monitor the RAID state When a RAID controller fault is detected, a trap is sent. **NOTE:** From Junos Space Platform Release 16.1 onward, if you want to use the **Monitor RAID** option, you need to install **StorMan-7.31-18856.x86_64 .rpm** . For installation instructions, see "Installing StorMan RPM for Monitor RAID Functionality" on page 1253. **NOTE:** This field is not applicable to and is disabled for Junos Space Virtual Appliances.	Selected	Cleared
Disk Usage %	When the percentage of the disk in use exceeds the configured disk usage percentage, an alarm is triggered.	5	5

Table 152: SNMP Configuration *(continued)*

Setting	Explanation	Recommended Settings	Default Value
System Load (1 min)	When the average system load (over 1 minute) exceeds the configured value, an alarm is triggered.	4	4
System Load (5 min)	When the average system load (over 5 minutes) exceeds the configured value, an alarm is triggered.	4	4
System Load (15 min)	When the average system load (over 15 minutes) exceeds the configured value, an alarm is triggered.	4	4
System Location	Location of the fabric node	Actual geographical or other location	unknown
System Contact	E-mail address to which the system sends notifications	E-mail address of actual person	root <root@localhost>
Disk Mount Path	Disk mount path that is to be monitored **NOTE:** This field is disabled if the **Monitor All Disks** field is selected.	Actual path, if available	/
CPU Max Temp (mC)	When the temperature exceeds the configured value, an alarm is triggered. **NOTE:** This field is applicable only to the Junos Space hardware appliances (JA2500).	50000	50000
CPU Min Fan (RPM)	When the CPU fan speed goes below the configured value, an alarm is triggered. **NOTE:** This field is applicable only to the Junos Space hardware appliances (JA2500).	1000	1000

Table 152: SNMP Configuration *(continued)*

Setting	Explanation	Recommended Settings	Default Value
CPU Min Voltage (mV)	When the CPU voltage goes below the configured value, an alarm is triggered. **NOTE:** This field is applicable only to the Junos Space hardware appliances (JA2500).	1000	1000

4. Select **Confirm** to apply the SNMP configuration changes to the node, or select **Cancel** if you do not want to make any changes to the SNMP configuration.

Table 153 shows the configuration parameters for monitoring disk usage.

Table 153: SNMP Configuration Parameters: Monitoring Disk Usage

Monitoring Disk Usage

Table 153: SNMP Configuration Parameters: Monitoring Disk Usage *(continued)*

Monitoring Disk Usage
Parameter: **Disk Usage (%)** Default: 5% When the free disk space is greater than the configured threshold, the trap shown in Figure 61 is generated.

Figure 61: Disk Usage Threshold Is Normal

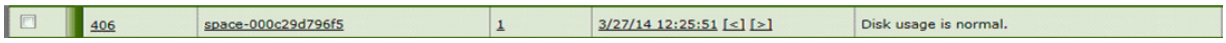
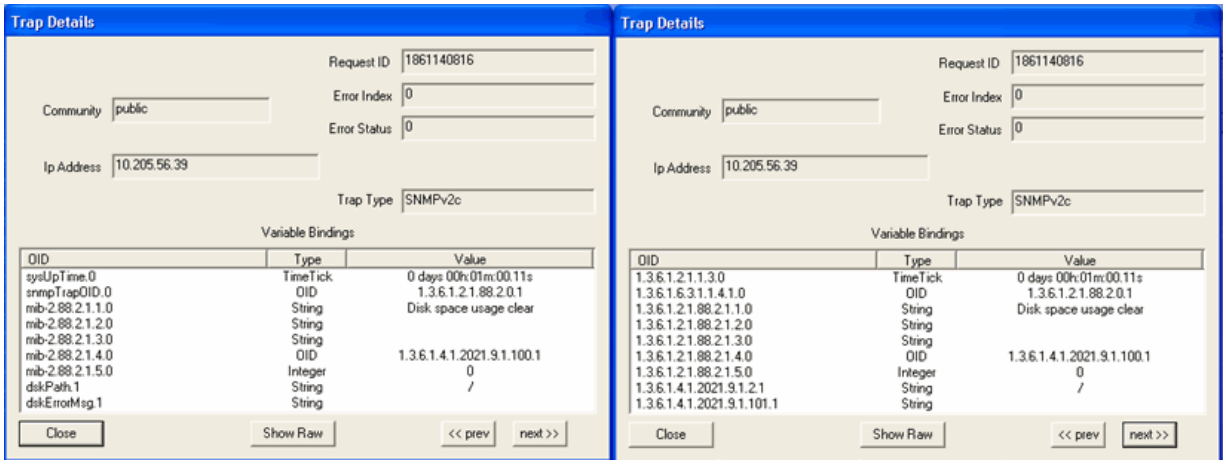


Figure 62 shows the OID details for the trap generated when disk usage is normal.

Figure 62: Trap Details When Disk Usage Normal



When the free disk space is less than the configured threshold, the trap shown in Figure 63 is generated.

Figure 63: Disk Usage Threshold Exceeds Configured Threshold

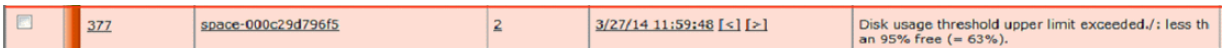


Figure 64 shows the OID details for the trap generated when disk usage exceeds the configured threshold.

Figure 64: Trap Details When DIsk Usage Exceeds Configured Threshold

Table 153: SNMP Configuration Parameters: Monitoring Disk Usage *(continued)*

Monitoring Disk Usage

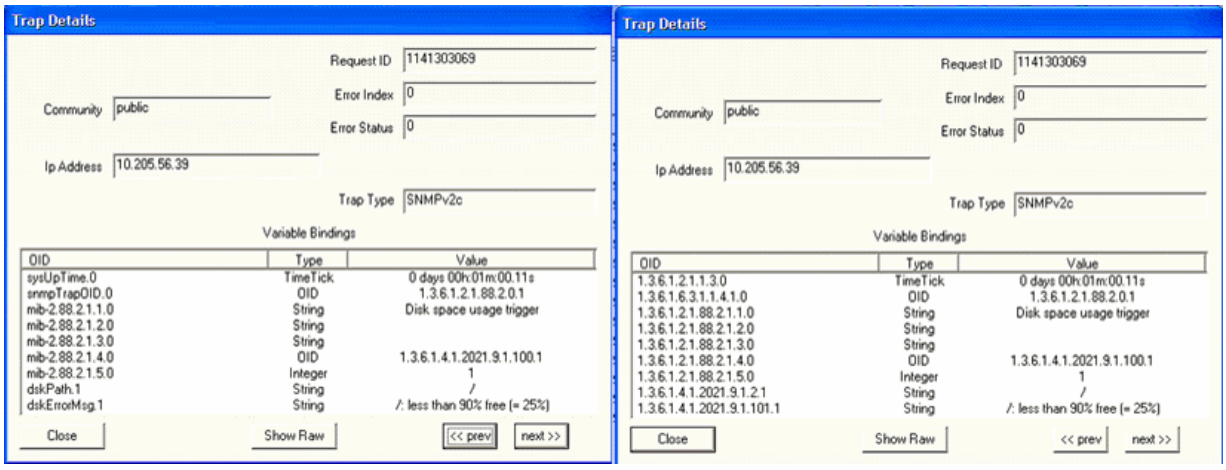


Table 154 shows the configuration parameters for monitoring the CPU load average.

Table 154: SNMP Configuration Parameters: Monitoring the CPU Load Average

Monitoring the CPU Load Average (System Load)

Table 154: SNMP Configuration Parameters: Monitoring the CPU Load Average *(continued)*

Monitoring the CPU Load Average (System Load)
Parameter: **CPU Load (1 min, 5 min, 15 min)** Default Threshold Value: 4 When the CPU Load Average threshold is less than or equal to the configured threshold limit, the trap shown in Figure 65 is generated:

Figure 65: CPU Load Average Threshold Is Normal

Figure 66 shows the OID details for the trap generated when the CPU load is normal.

Figure 66: Trap Details When CPU Load Average Threshold Is Normal

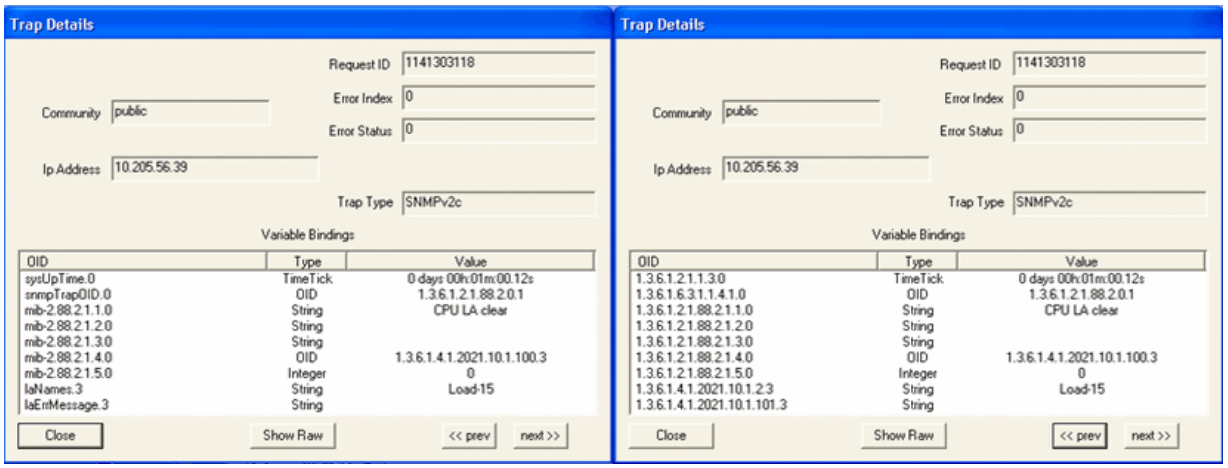


Figure 67 shows the traps generated when the 15 minute, 5 minute, or 1 minute CPU Load Average threshold is exceeded.

Figure 67: CPU Load Average Threshold – Upper Limit Exceeded

Figure 68 shows the OID details for the trap generated when the CPU load 5 minute average exceeds the threshold.

Figure 68: Trap Details When CPU Load 5 Minute Average Exceeds Threshold

Table 154: SNMP Configuration Parameters: Monitoring the CPU Load Average *(continued)*

Monitoring the CPU Load Average (System Load)

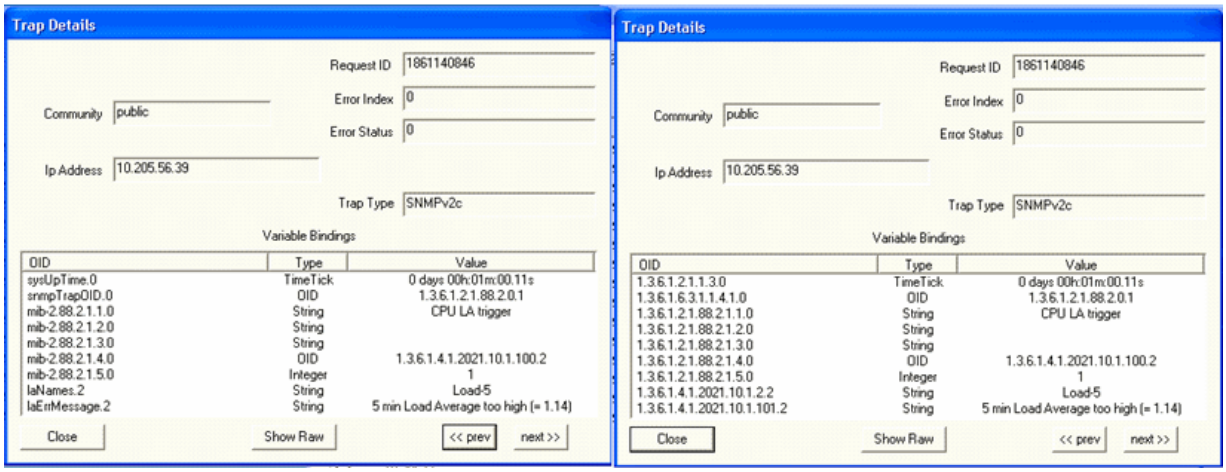


Table 155 shows monitoring processes for the Junos Space Network Management Platform.

Table 155: SNMP Configuration Parameters: Monitoring Processes

Monitoring Processes

Table 155: SNMP Configuration Parameters: Monitoring Processes *(continued)*

Monitoring Processes
Parameter: Node Management Agent (NMA) When the NMA process is up, the trap shown in Figure 69 is generated:

Figure 69: NMA Is Up

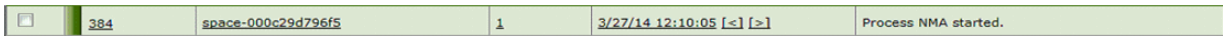
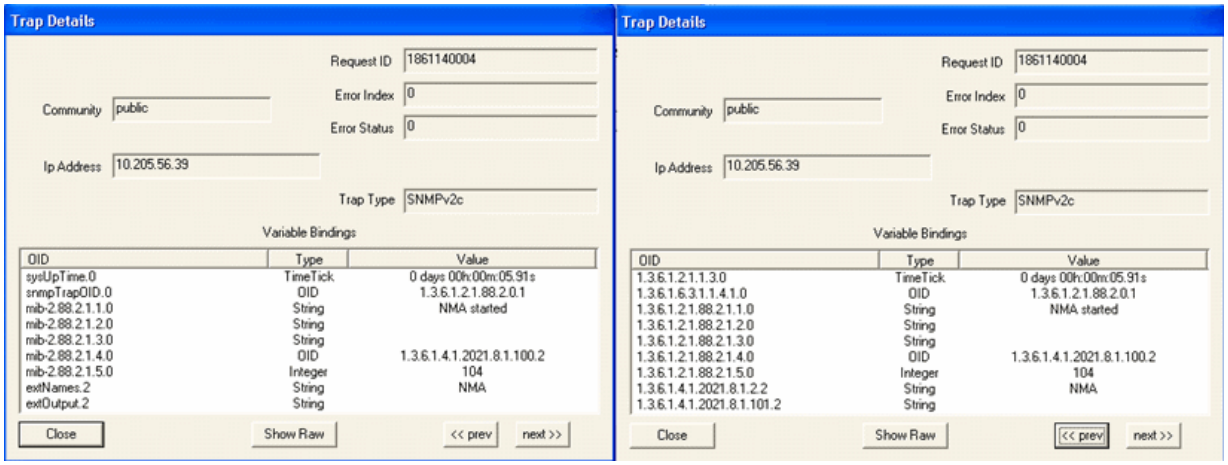


Figure 70 shows the OID details for the trap generated when the NMA process is up.

Figure 70: Trap Details When NMA Is Up



When the NMA process is down, the trap shown in Figure 71 is generated:

Figure 71: NMA is Down

Figure 72 shows the OID details for the trap generated when the NMA process is down.

Figure 72: Trap Details When NMA is Down

Table 155: SNMP Configuration Parameters: Monitoring Processes *(continued)*

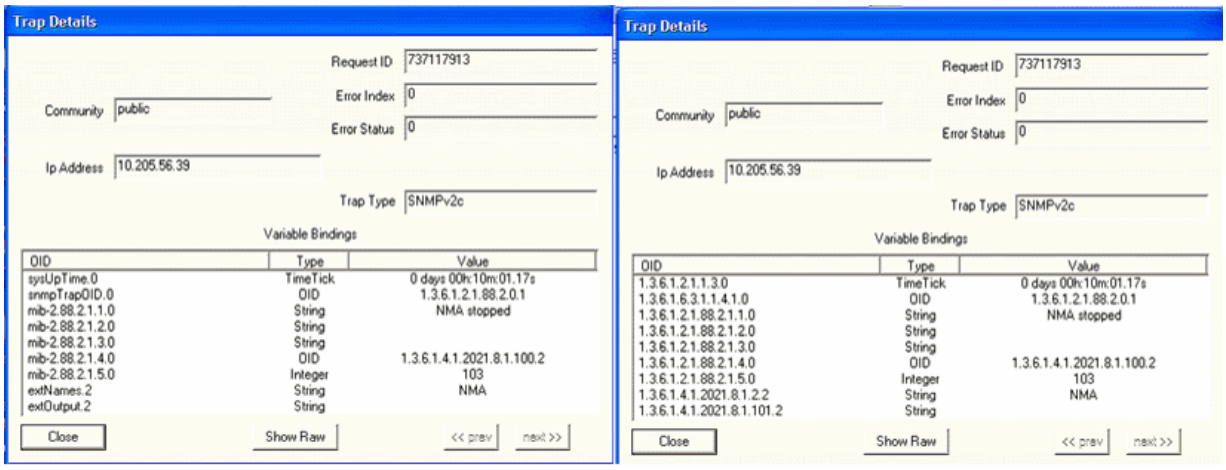
Monitoring Processes


Table 155: SNMP Configuration Parameters: Monitoring Processes *(continued)*

Monitoring Processes

Table 155: SNMP Configuration Parameters: Monitoring Processes *(continued)*

Monitoring Processes

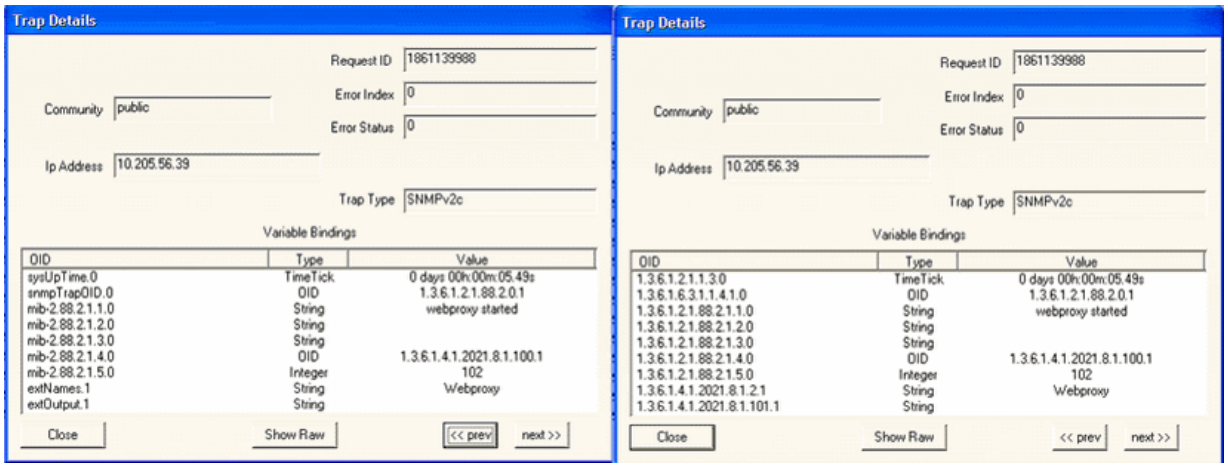
Parameter: Webproxy

When the WebProxy process is up, the trap shown in Figure 73 is generated:

Figure 73: WebProxy Is Up

Figure 74 shows the OID details for the trap generated when the WebProxy process is up.

Figure 74: Trap Details When WebProxy Is Up



When the WebProxy process is down, the trap shown in Figure 75 is generated:

Figure 75: WebProxy Is Down

Figure 76 shows the OID details for the trap generated when the WebProxy is down.

Figure 76: Trap Details When WebProxy Is Down

Table 155: SNMP Configuration Parameters: Monitoring Processes *(continued)*

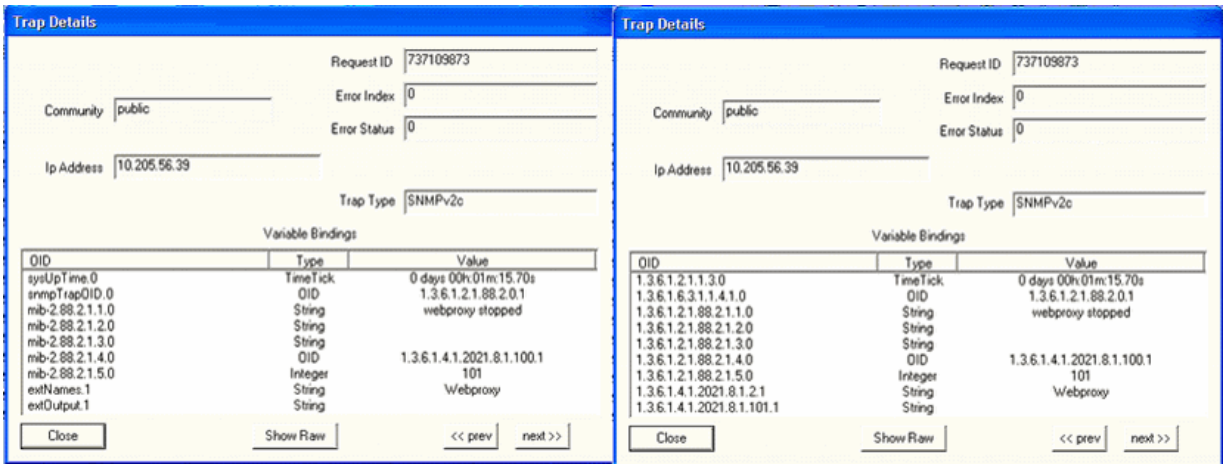
Monitoring Processes


Table 155: SNMP Configuration Parameters: Monitoring Processes *(continued)*

Monitoring Processes

Table 155: SNMP Configuration Parameters: Monitoring Processes *(continued)*

Monitoring Processes
Parameter: JBoss When the JBoss process is up, the trap shown in Figure 77 is generated:

Figure 77: JBoss Is Up

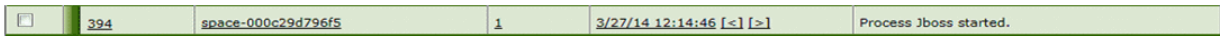
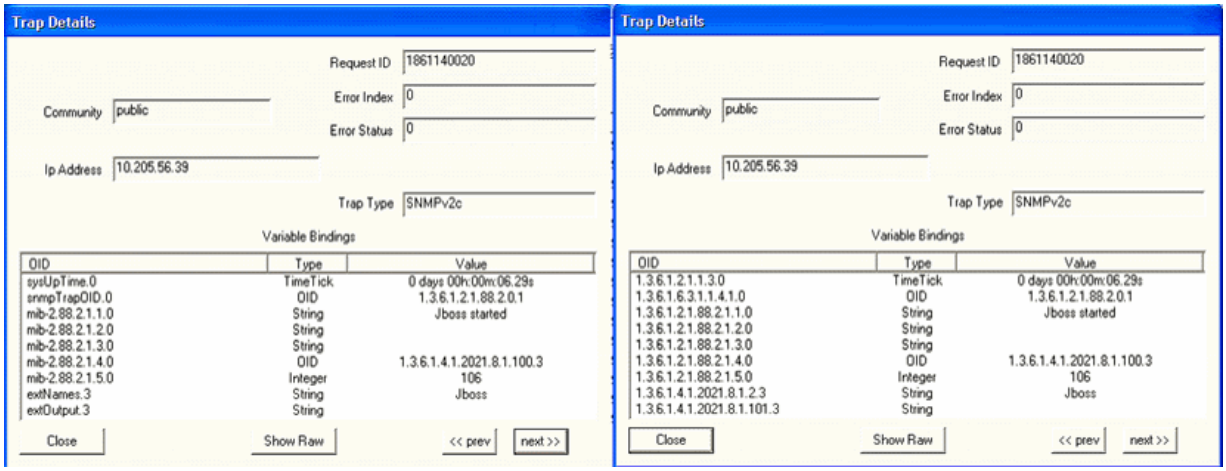


Figure 78 shows the OID details for the trap generated when the JBoss process is up.

Figure 78: Trap Details When JBoss Is Up



When the JBoss process is down, the trap shown in Figure 79 is generated:

Figure 79: JBoss Is Down

Figure 80 shows the OID details for the trap generated when JBoss is down.

Figure 80: Trap Details When JBoss Is Down

Table 155: SNMP Configuration Parameters: Monitoring Processes *(continued)*

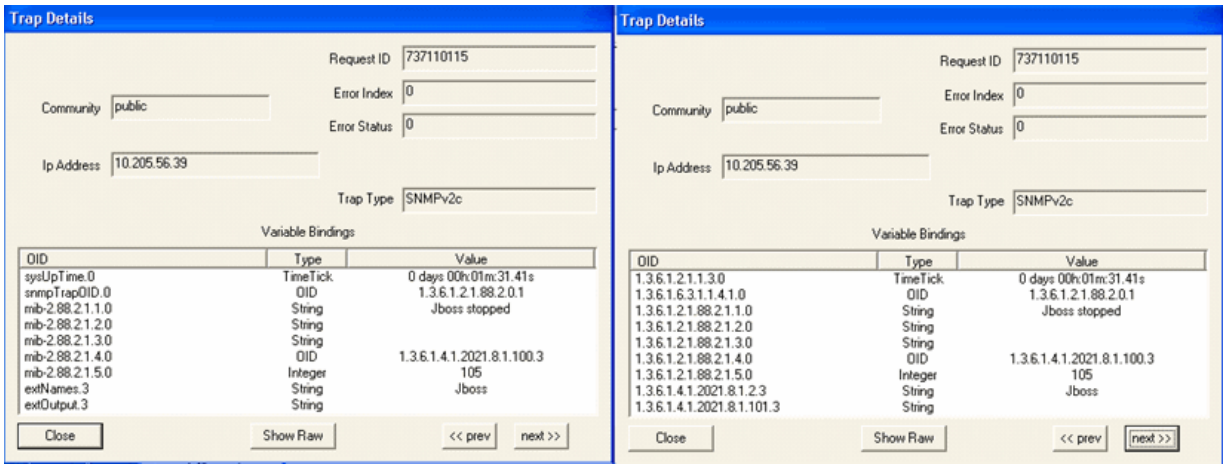
Monitoring Processes


Table 155: SNMP Configuration Parameters: Monitoring Processes *(continued)*

Monitoring Processes

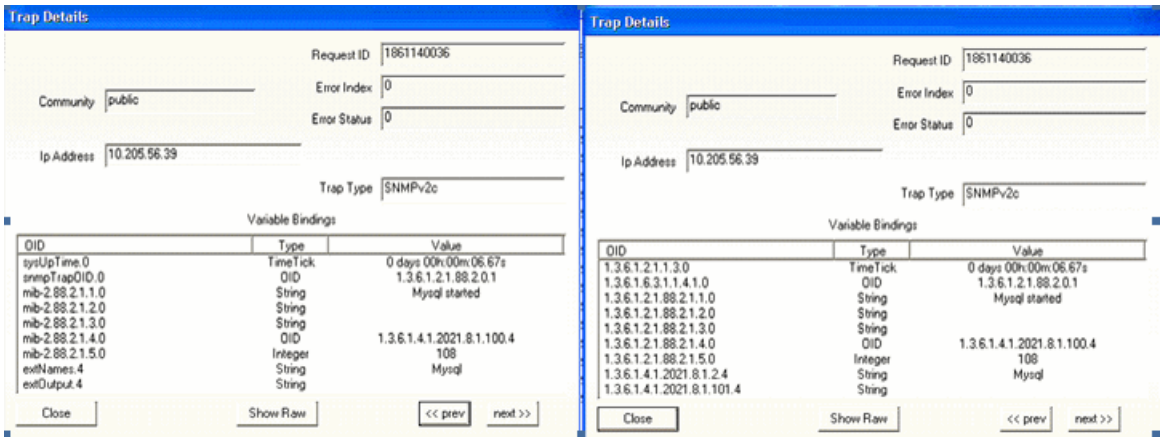
Table 155: SNMP Configuration Parameters: Monitoring Processes *(continued)*

Monitoring Processes
Parameter: Mysql When the Mysql process is up, the trap shown in Figure 81 is generated:

Figure 81: Mysql Is Up

Figure 82 shows the OID details for the trap generated when the Mysql process is up.

Figure 82: Trap Details When Mysql Is Up



When the Mysql process is down, the trap shown in Figure 83 is generated:

Figure 83: Mysql Is Down

Figure 84 shows the OID details for the trap generated when the Mysql process is down.

Figure 84: Trap Details When Mysql Is Down

Table 155: SNMP Configuration Parameters: Monitoring Processes *(continued)*

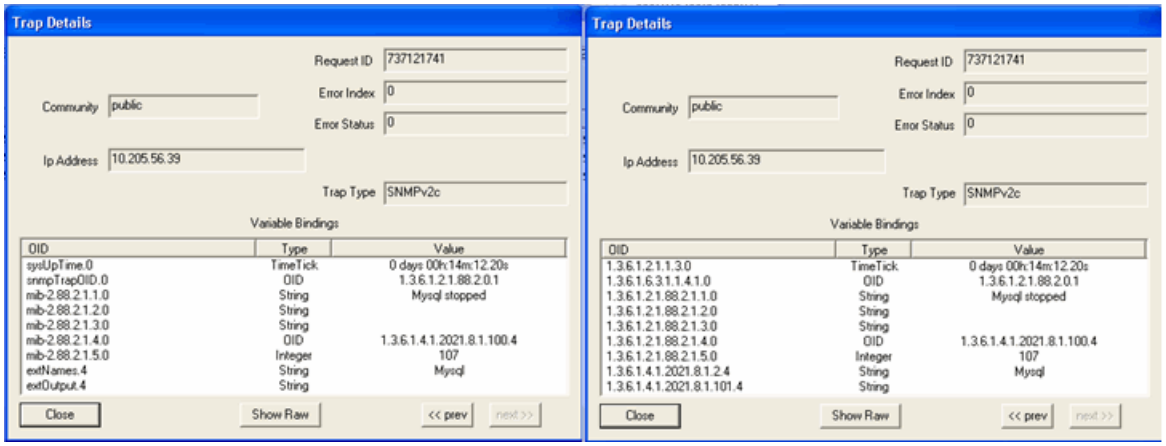
Monitoring Processes


Table 155: SNMP Configuration Parameters: Monitoring Processes *(continued)*

Monitoring Processes

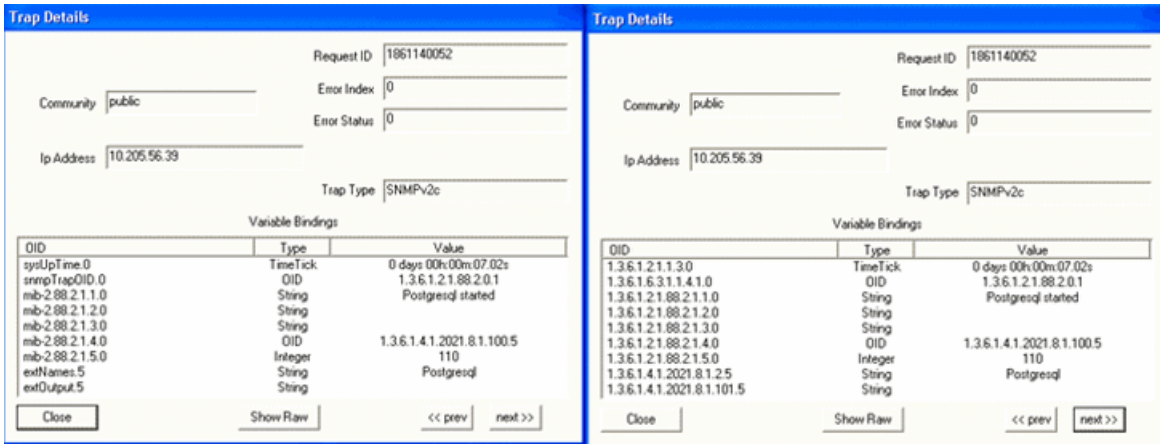
Table 155: SNMP Configuration Parameters: Monitoring Processes *(continued)*

Monitoring Processes
Parameter: Postgresql
When the Postgresql process is up, the trap shown in Figure 85 is generated:

Figure 85: Postgresql Is Up

Figure 86 shows the OID details for the trap generated when the Postgresql process is up.

Figure 86: Trap Details When Postgresql Is Up



When the Postgresql process is down, the trap shown in Figure 87 is generated:

Figure 87: Postgresql Is Down

Figure 88 shows the OID details for the trap generated when the Postgresql process is up.

Figure 88: Trap Details When Postgresql Is Down

Table 155: SNMP Configuration Parameters: Monitoring Processes *(continued)*

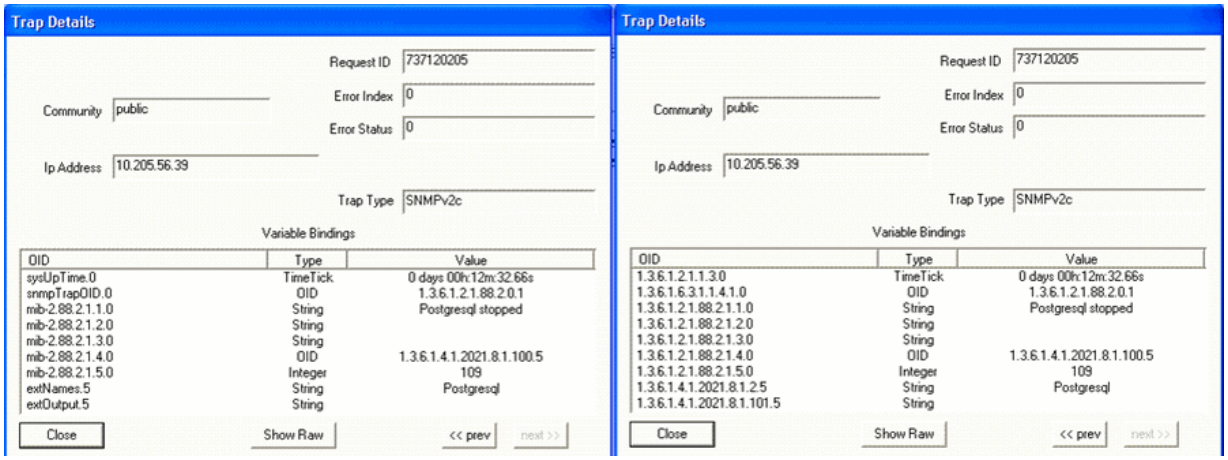
Monitoring Processes


Table 155: SNMP Configuration Parameters: Monitoring Processes *(continued)*

Monitoring Processes

Table 155: SNMP Configuration Parameters: Monitoring Processes *(continued)*

Monitoring Processes
Parameter: Free swap memory When the free swap memory is greater than the upper threshold limit, the trap shown in Figure 89 is generated:

Figure 89: Swap Memory Usage Is Normal

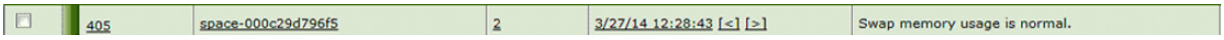
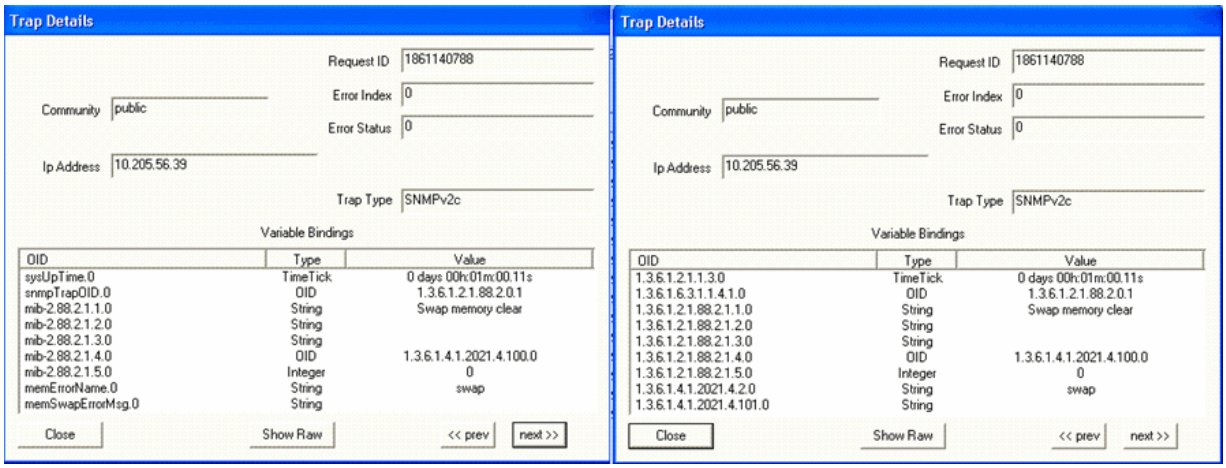


Figure 90 shows the OID details for the trap generated when swap memory usage is normal.

Figure 90: Trap Details When Swap Memory Is Normal



When the free swap memory is less than the upper threshold limit, the trap shown in Figure 91 is generated:

Figure 91: Swap Memory Usage Threshold Exceeds Upper Limit

Figure 92 shows the OID details for the trap generated when swap memory usage is exceeds upper limit.

Figure 92: Trap Details When Swap Memory Usage Exceeds Upper Limit

Table 155: SNMP Configuration Parameters: Monitoring Processes *(continued)*

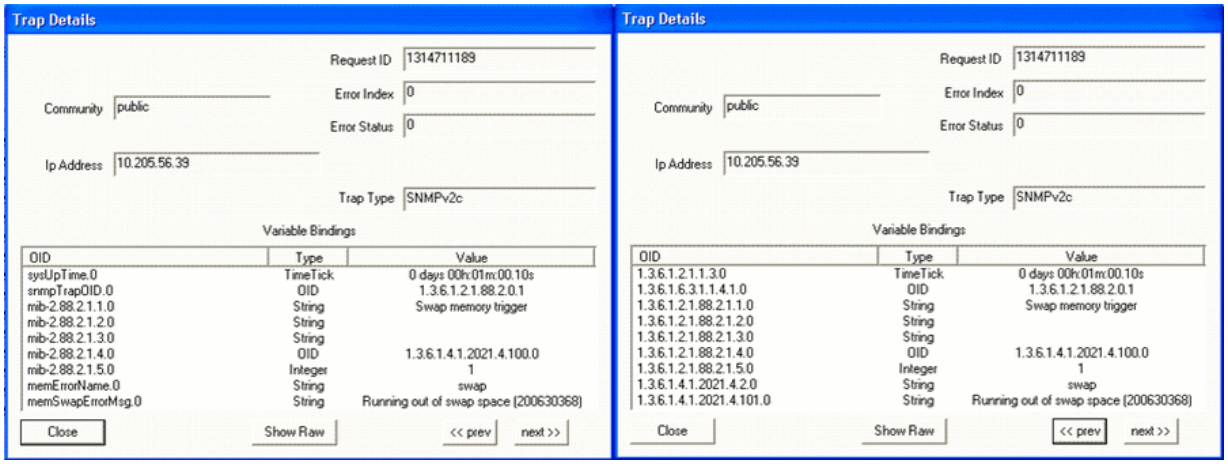
Monitoring Processes


Table 156 shows the configuration parameters for monitoring Junos Space Network Management Platform hardware.

Table 156: SNMP Configuration Parameters: Monitoring Linux Hardware

Monitoring Linux Hardware
NOTE: LM-SENSORS-MIB is not supported by the Junos Space Virtual Appliance, but only by the Junos Space Appliance. Therefore the threshold settings of CPU Max Temp (mC), CPU Min Fan (RPM) and CPU Min Voltage (mV) will not trigger any traps in the virtual appliance.

Table 156: SNMP Configuration Parameters: Monitoring Linux Hardware *(continued)*

Monitoring Linux Hardware

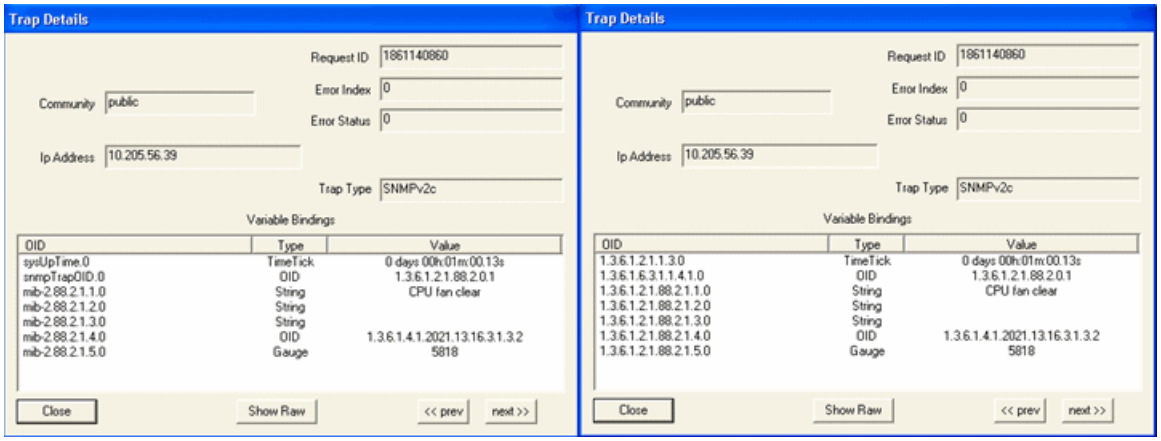
Table 156: SNMP Configuration Parameters: Monitoring Linux Hardware *(continued)*

Monitoring Linux Hardware
Parameter: **CPU min FAN (rpm)** Default Threshold Value: 1500 When the CPU fan speed is greater than the configured threshold (minimum fan speed), the trap shown in Figure 93 is generated:

Figure 93: CPU Fan Speed Normal

Figure 94 shows the OID details for the trap generated when CPU fan speed is normal.

Figure 94: Trap Details When CPU Fan Speed Is Normal



When the CPU fan speed is less than the configured threshold (minimum fan speed), the trap shown in Figure 95 is generated:

Figure 95: CPU Fan Speed Is Below the Configured Threshold

Figure 96 shows the OID details for the trap generated when CPU fan speed lower than the configured threshold.

Figure 96: Trap Details When CPU Fan Speed Is Below the Configured Threshold

Table 156: SNMP Configuration Parameters: Monitoring Linux Hardware *(continued)*

Monitoring Linux Hardware

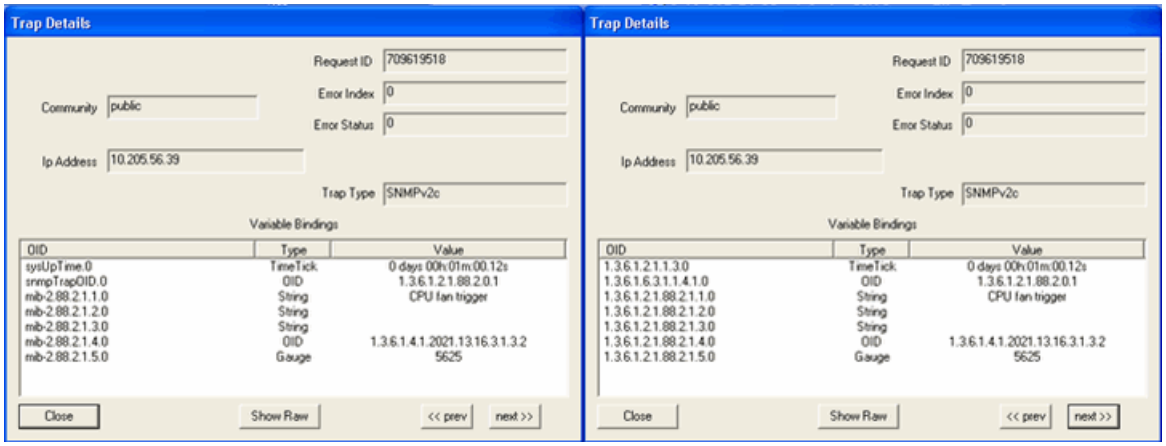


Table 156: SNMP Configuration Parameters: Monitoring Linux Hardware *(continued)*

Monitoring Linux Hardware

Table 156: SNMP Configuration Parameters: Monitoring Linux Hardware *(continued)*

Monitoring Linux Hardware

Parameter: **CPU min Voltage (mV)**

When the CPU voltage is greater than the configured value, the trap shown in Figure 97 is generated:

Figure 97: CPU Voltage Normal

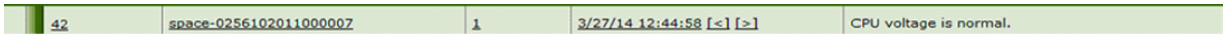
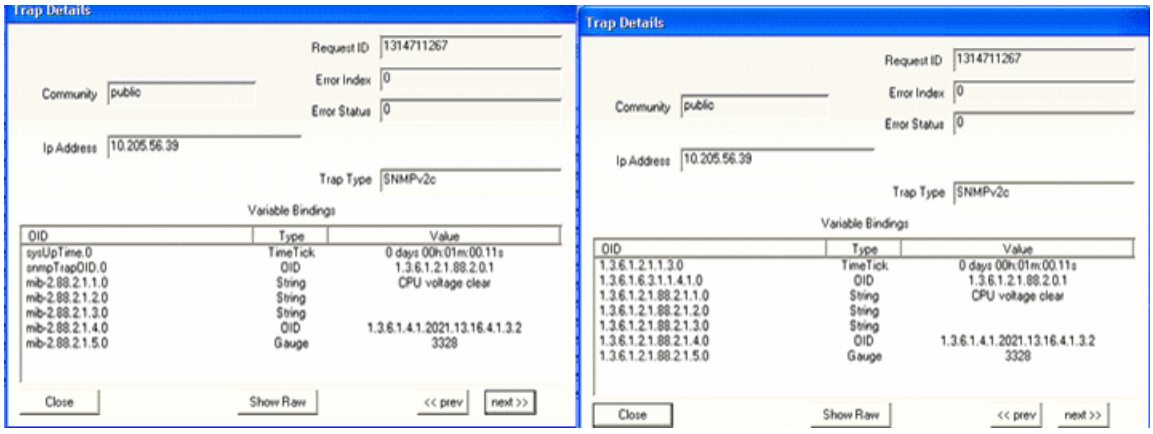


Figure 98 shows the OID details for the trap generated when CPU voltage is normal.

Figure 98: Trap Details When CPU Voltage Is Normal



Default Threshold Value: 1000

When the CPU voltage is lower than the configured value, the trap shown in Figure 99 is generated:

Figure 99: CPU Voltage Is Lower Than Configured Threshold

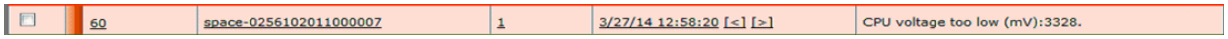


Figure 100 shows the OID details for the trap generated when CPU voltage is lower than the configured threshold.

Figure 100: Trap Details When CPU Voltage Is Lower Than Configured Threshold

Table 156: SNMP Configuration Parameters: Monitoring Linux Hardware *(continued)*

Monitoring Linux Hardware

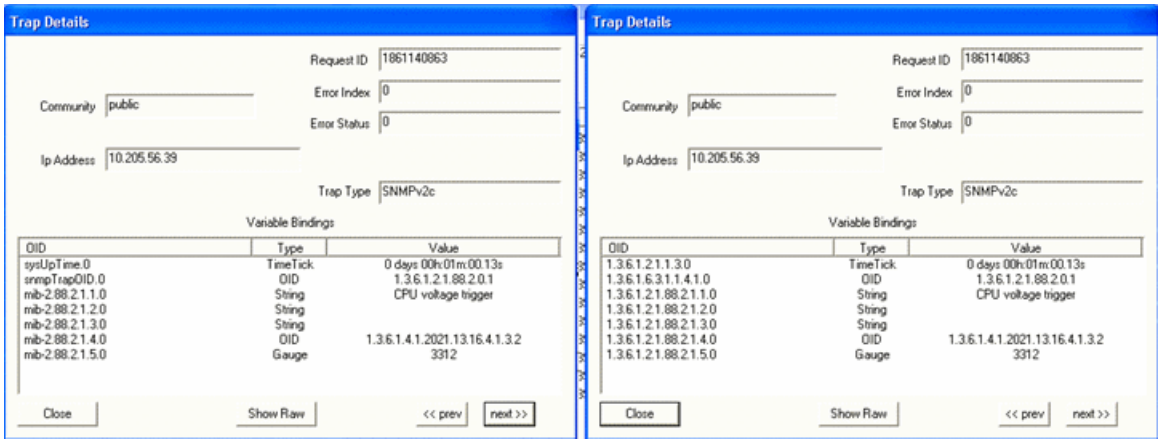


Table 156: SNMP Configuration Parameters: Monitoring Linux Hardware *(continued)*

Monitoring Linux Hardware

Table 156: SNMP Configuration Parameters: Monitoring Linux Hardware *(continued)*

Monitoring Linux Hardware
Parameter: **CPU Temperature** When the CPU temperature is lower than the configured threshold, the trap shown in Figure 101 is generated:

Figure 101: CPU Temperature Normal

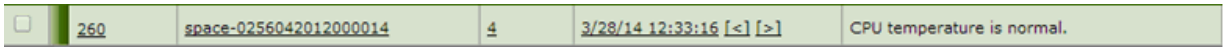
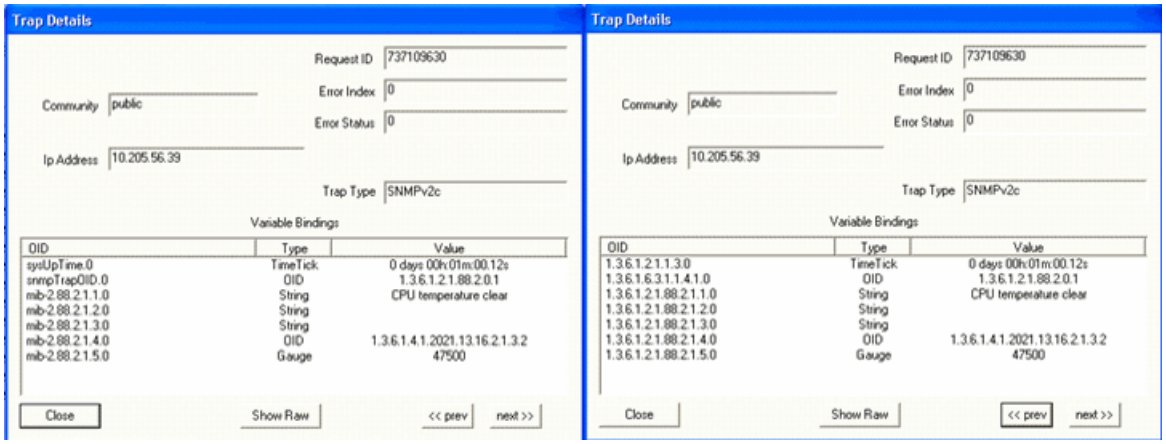


Figure 102 shows the OID details for the trap generated when CPU temperature is normal.

Figure 102: Trap Details When CPU Temperature Is Normal



When the CPU temperature exceeds the configured threshold, the trap shown in Figure 103 is generated:

Figure 103: CPU Temperature Exceeds The Configured Threshold

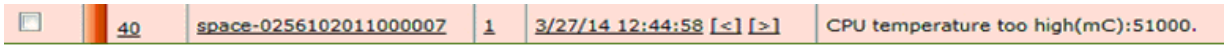


Figure 104 shows the OID details for the trap generated when CPU temperature is higher than the configured threshold.

Figure 104: Trap Details When CPU Temperature Exceeds The Configured Threshold

Table 156: SNMP Configuration Parameters: Monitoring Linux Hardware *(continued)*

Monitoring Linux Hardware

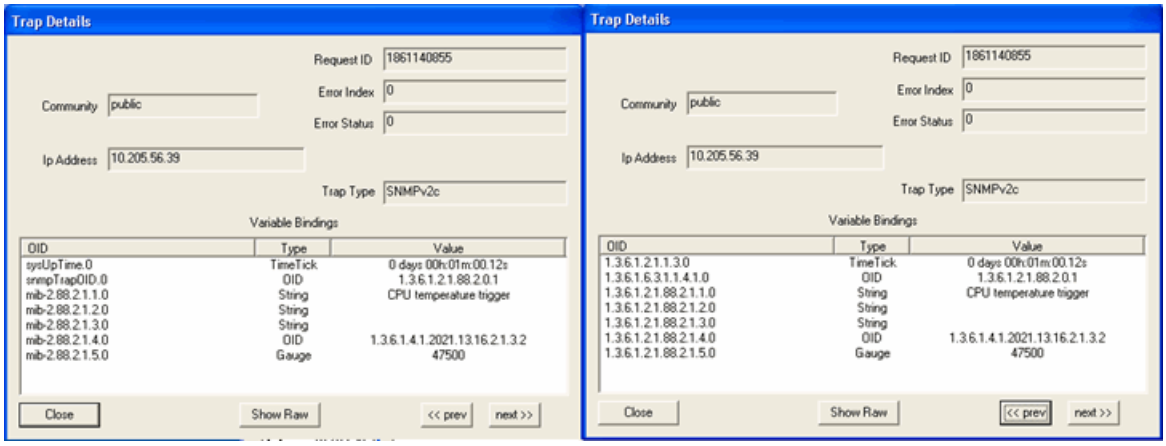


Table 157 shows the configuration parameters for monitoring fabric health.

Table 157: SNMP Configuration Parameters: Monitoring Fabric Health

Monitoring Fabric Health

Table 157: SNMP Configuration Parameters: Monitoring Fabric Health *(continued)*

Table 157: SNMP Configuration Parameters: Monitoring Fabric Health *(continued)*

Parameter: Junos Space Node

When a Junos Space node is up, the trap shown in Figure 105 is generated:

Figure 105: Junos Space Node is Up

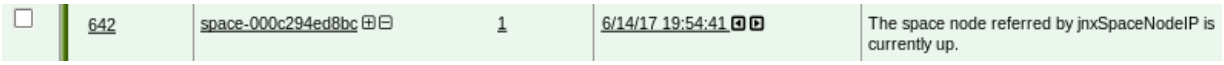
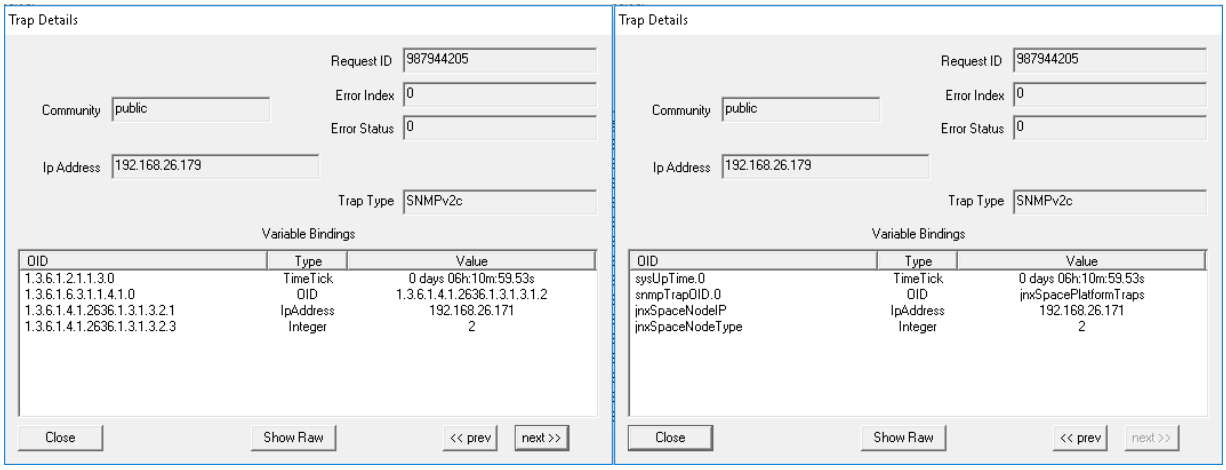


Figure 106 shows the OID details for the trap generated when a Junos Space node is up.

Figure 106: Trap Details When Junos Space Node Is Up



When a Junos Space node is down, the trap shown in Figure 107 is generated:

Figure 107: Junos Space Node is Down

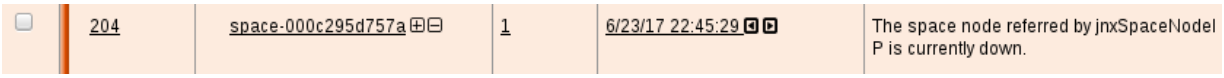
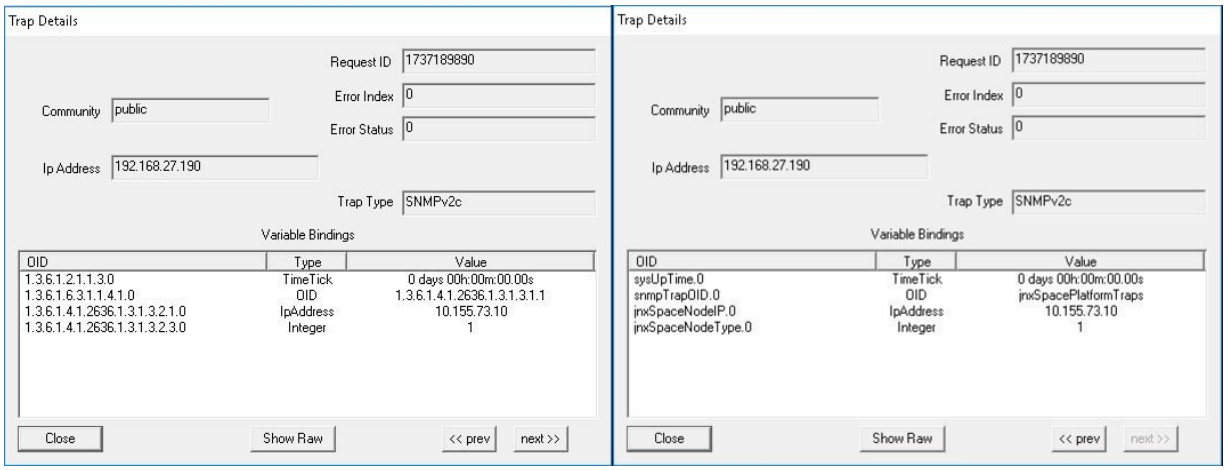


Figure 108 shows the OID details for the trap generated when a Junos Space node is down.

Figure 108: Trap Details When Junos Space Node is Down

Table 157: SNMP Configuration Parameters: Monitoring Fabric Health *(continued)*



Parameter: Junos Space Node Removal

When a Junos Space node is removed from the fabric, the trap shown in Figure 109 is generated:

Figure 109: Junos Space Node Is Removed

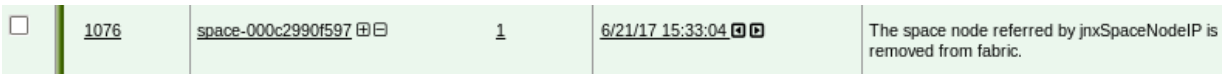


Figure 110 shows the OID details for the trap generated when a Junos Space node is removed..

Figure 110: Trap Details When Junos Space Node Is Removed

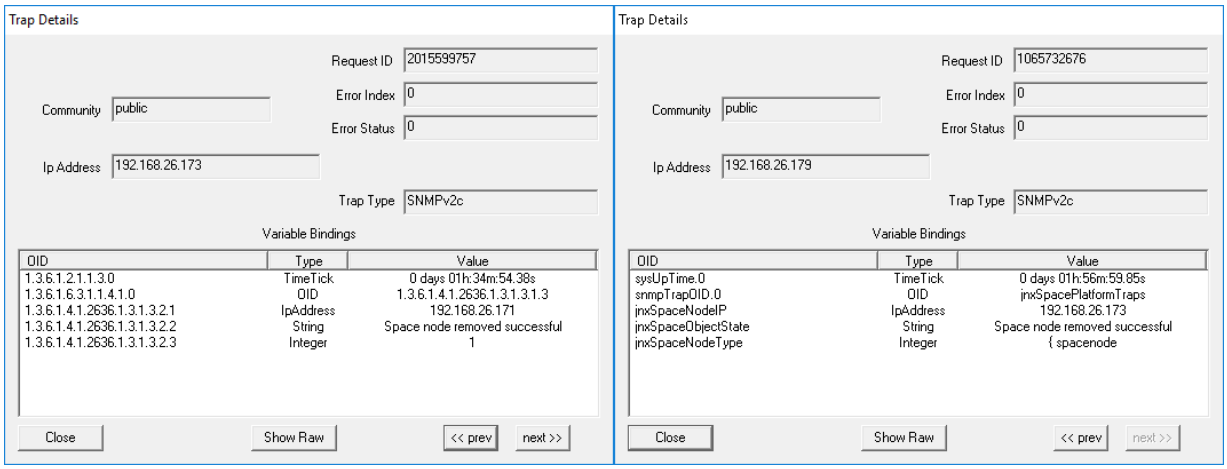


Table 157: SNMP Configuration Parameters: Monitoring Fabric Health *(continued)*

Parameter: JBoss Multi-Primary Detected

When there is more than one JBoss AppLogic primary node detected in the cluster, the trap shown in Figure 111 is generated:

Figure 111: JBoss Multi-Primary Detected

[xref target has no title] shows the OID details for the trap generated when there is more than one JBoss AppLogic primary node detected in the cluster.

Figure 112: Trap Details When JBoss Multi-Primary Is Detected

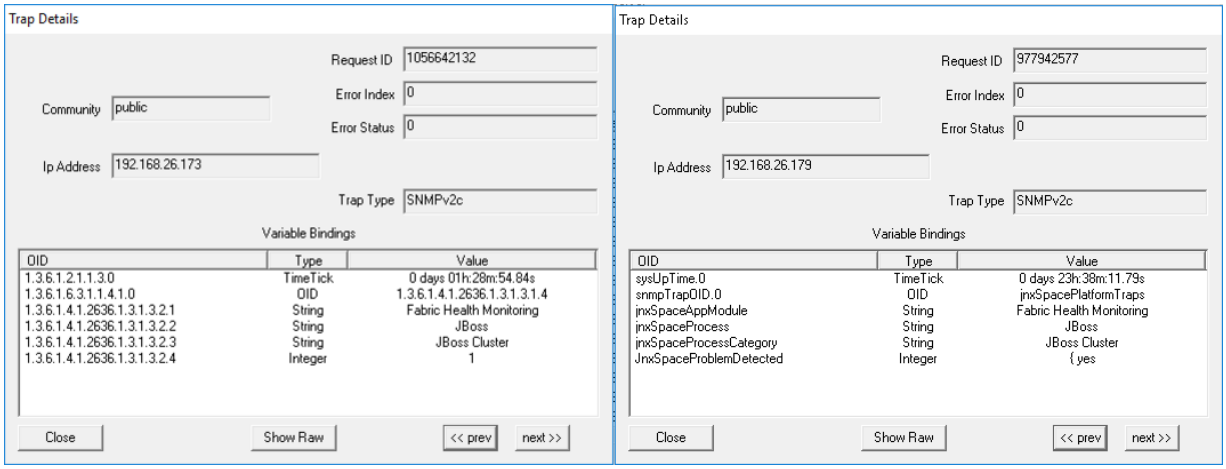


Table 157: SNMP Configuration Parameters: Monitoring Fabric Health *(continued)*

Parameter: VIP Bind Issue Detected in JBoss Node(s)

When VIP Bind issue is detected in JBoss node(s), the trap shown in Figure 113 is generated:

Figure 113: VIP Bind Issue Detected In JBoss Node(s)

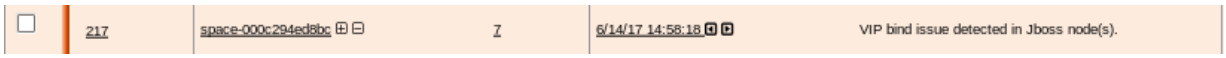


Figure 114 shows the OID details for the trap generated when VIP Bind issue is detected in JBoss node(s).

Figure 114: Trap Details When VIP Bind Issue Is Detected In JBoss Node(s)

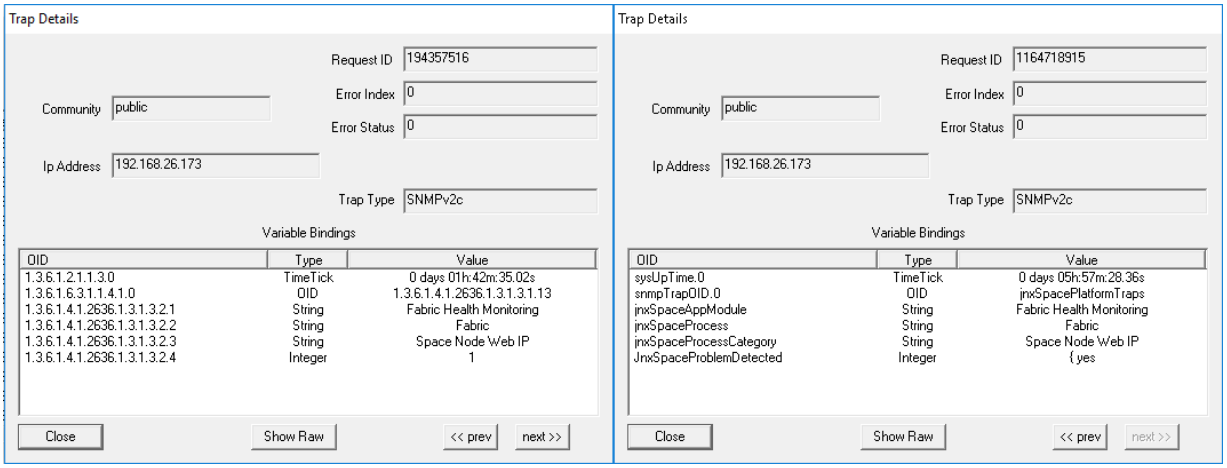


Table 157: SNMP Configuration Parameters: Monitoring Fabric Health *(continued)*

Parameter: VIP Bind Issue Detected in Database Node(s)

When VIP Bind issue is detected in Database node(s), the trap shown in Figure 115 is generated:

Figure 115: VIP Bind Issue Detected In Database Node(s)

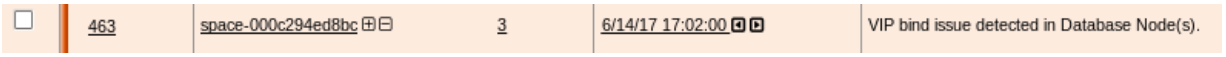


Figure 116 shows the OID details for the trap generated when VIP Bind issue is detected in Database node(s).

Figure 116: Trap Details When VIP Bind Issue Is Detected In Database Node(s)

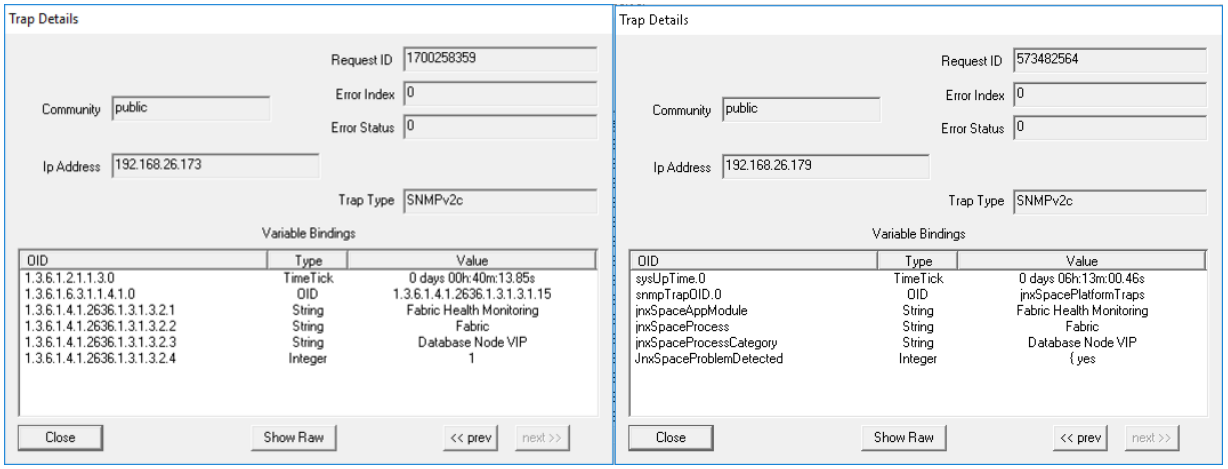


Table 157: SNMP Configuration Parameters: Monitoring Fabric Health *(continued)*

Parameter: VIP Bind Issue Detected in FMPM Node(s)

When VIP Bind issue is detected in FMPM node(s), the trap shown in Figure 117 is generated:

Figure 117: VIP Bind Issue Detected In FMPM Node(s)

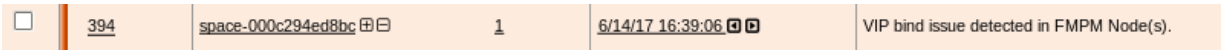


Figure 118 shows the OID details for the trap generated when VIP Bind issue is detected in FMPM node(s).

Figure 118: Trap Details When VIP Bind Issue Is Detected In FMPM Node(s)

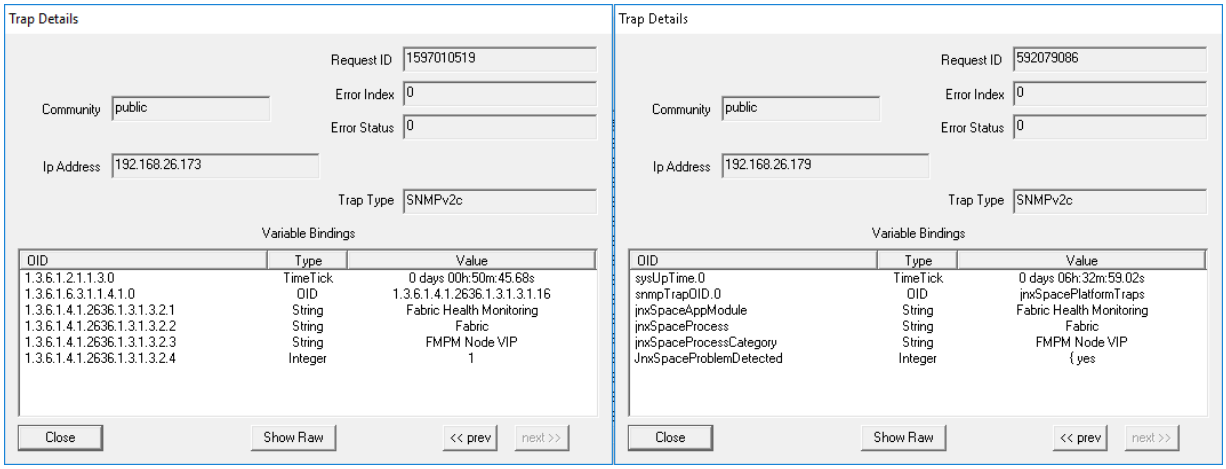


Table 157: SNMP Configuration Parameters: Monitoring Fabric Health *(continued)*

Parameter: Fabric Monitoring Process Inactive

When fabric monitoring process is inactive, the trap shown in Figure 119 is generated:

Figure 119: Fabric Monitoring Process Inactive

Figure 120 shows the OID details for the trap generated when fabric monitoring process is inactive.

Figure 120: Trap Details When Fabric Monitoring Process Is Inactive

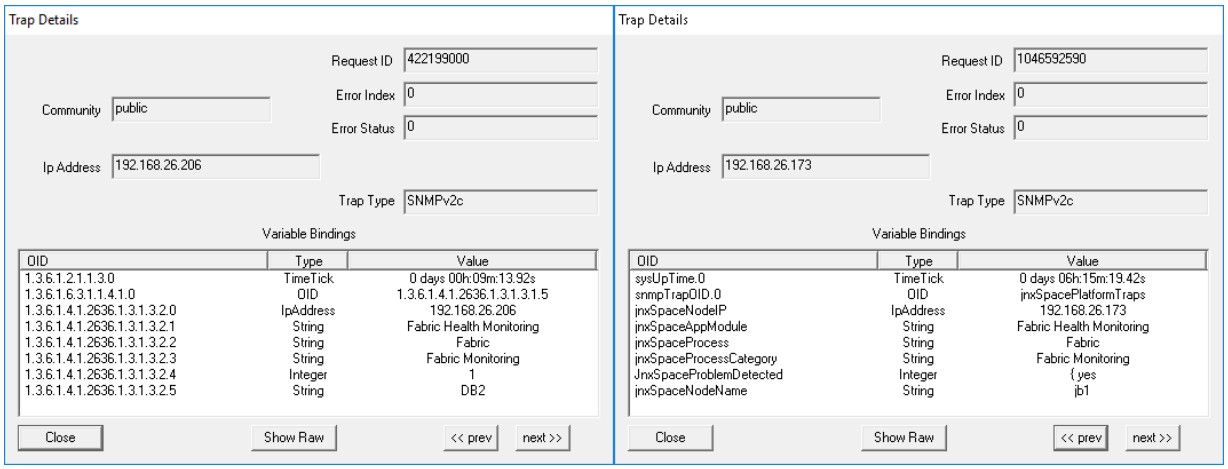


Table 157: SNMP Configuration Parameters: Monitoring Fabric Health *(continued)*

Parameter: Tables Exceed Size Limit

When one or more tables in the MySQL database exceed the size limit of 10 GB, the trap shown in Figure 121 is generated:

Figure 121: Tables Exceed Size Limit

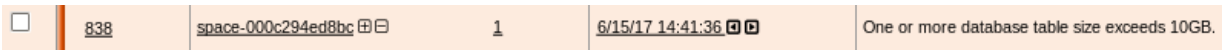


Figure 122 shows the OID details for the trap generated when one or more tables in the MySQL database exceed the size limit of 10 GB.

Figure 122: Trap Details When Tables Exceed Size Limit

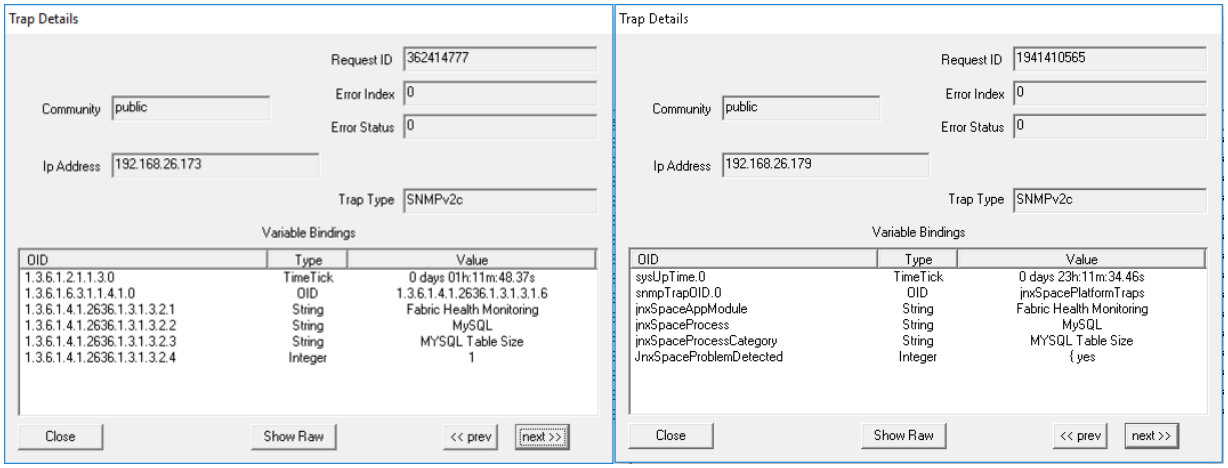


Table 157: SNMP Configuration Parameters: Monitoring Fabric Health *(continued)*

Parameter: Device Session Count Exceeds Threshold Limit

When the device session count exceeds the threshold limit, the trap shown in Figure 123 is generated:

Figure 123: Device Session Count Exceeds Threshold Limit

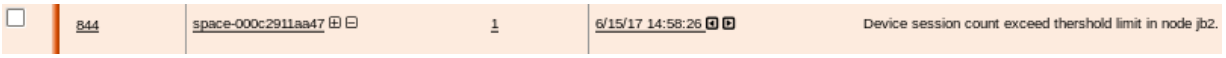


Figure 124 shows the OID details for the trap generated when the device session count exceeds the threshold limit.

Figure 124: Trap Details When Device Session Count Exceeds Threshold Limit

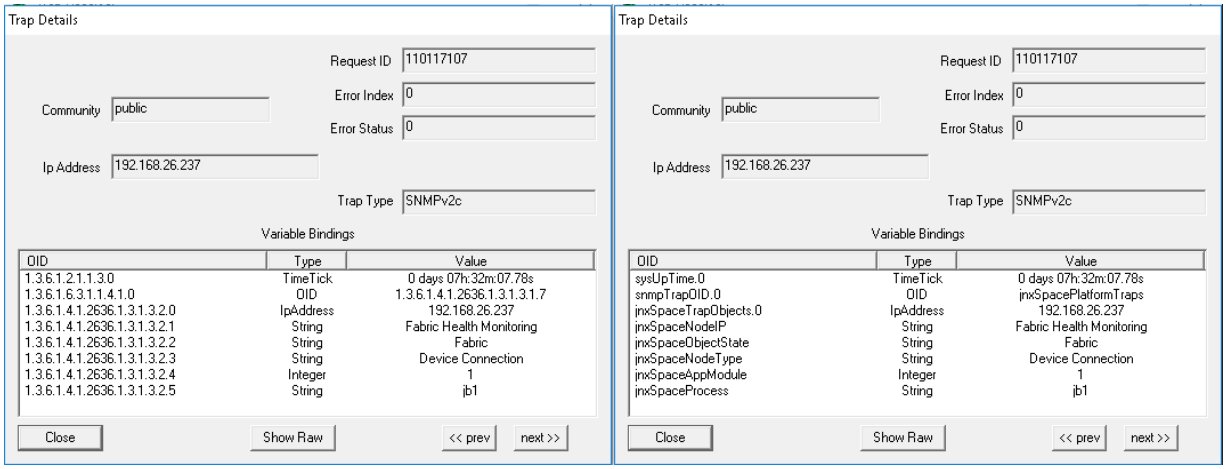


Table 157: SNMP Configuration Parameters: Monitoring Fabric Health *(continued)*

Parameter: HPROF Availability

When Heap and CPU Profiling Agent (HPROF) files are detected on a Junos Space node, the trap shown in Figure 125 is generated:

Figure 125: HPROF Availability

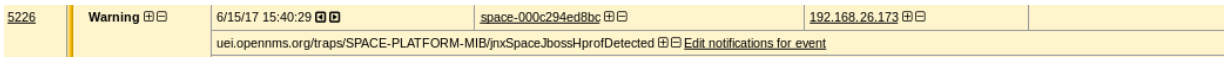


Figure 126 shows the OID details for the trap generated when HPROF files are detected on a Junos Space node.

Figure 126: Trap Details When HPROF Files Are Available

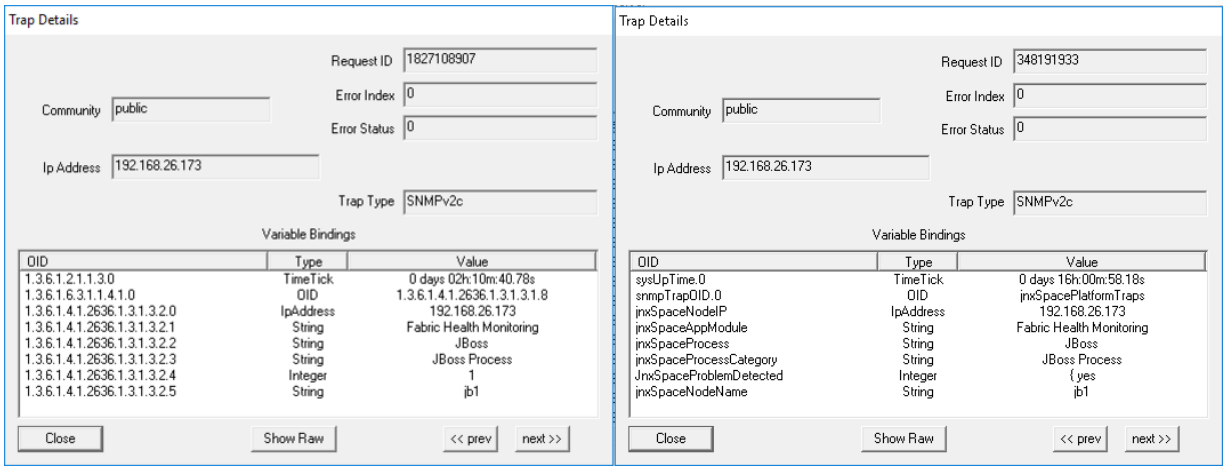


Table 157: SNMP Configuration Parameters: Monitoring Fabric Health *(continued)*

Parameter: JGroup Membership Issue Detected

When the removal of a JBoss node from JGroup is detected in the cluster, the trap shown in Figure 127 is generated:

Figure 127: JGroup Membership Issue Detected

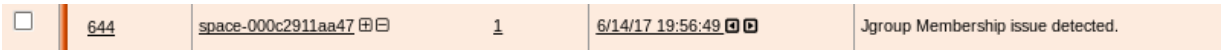


Figure 128 shows the OID details for the trap generated when the removal of a JBoss node from JGroup is detected in the cluster.

Figure 128: Trap Details When JGroup Membership Issue Detected

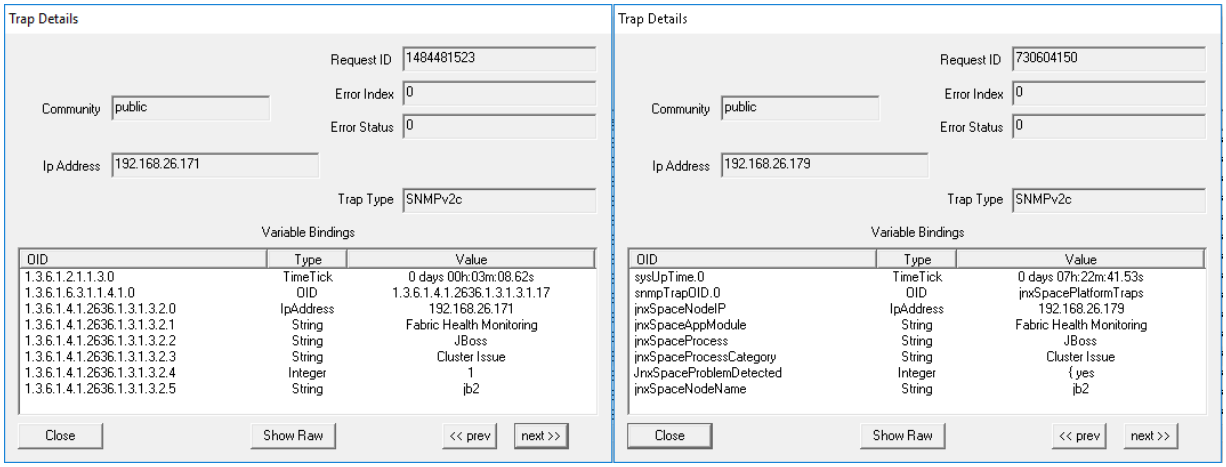


Table 157: SNMP Configuration Parameters: Monitoring Fabric Health *(continued)*

Parameter: MySQL In Out Of Sync State

When a MySQL database synchronization issue is detected between nodes running the MySQL database, the trap shown in Figure 129 is generated:

Figure 129: MySQL In Out Of Sync State

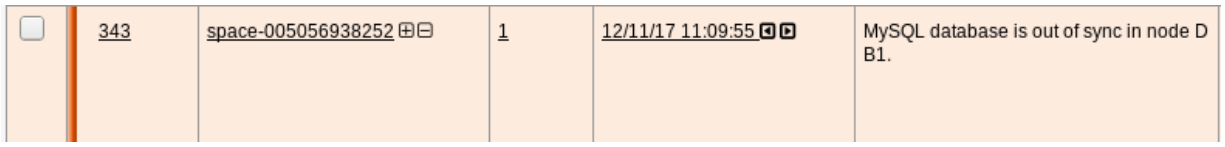


Figure 130 shows the OID details for the trap generated when a MySQL database synchronization issue is detected between nodes running the MySQL database.

Figure 130: Trap Details When MySQL Is In Out Of Sync State

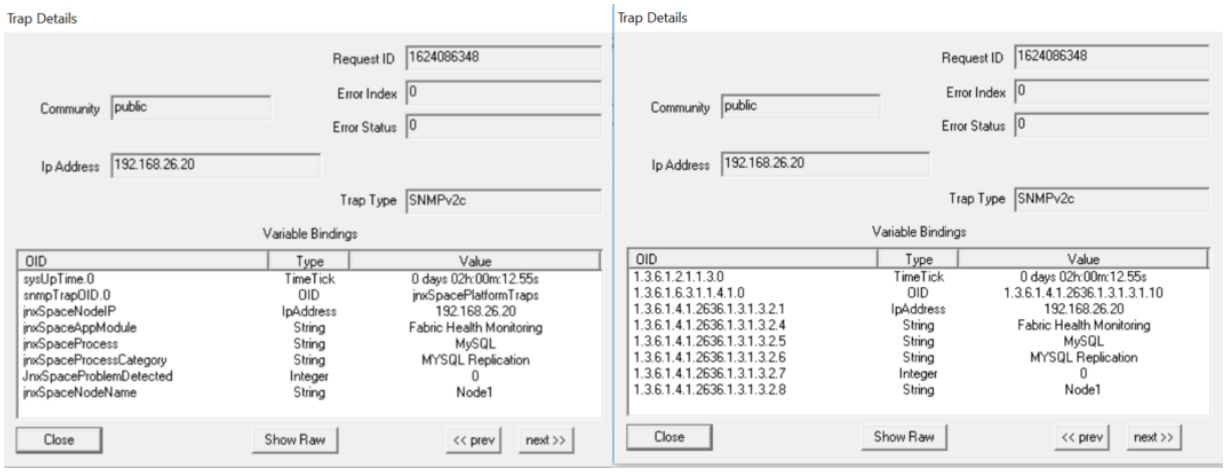


Table 157: SNMP Configuration Parameters: Monitoring Fabric Health *(continued)*

Parameter: File Intrusion Detection Monitoring

When changes in files or file permissions are detected, the trap shown in Figure 131 is generated.

Figure 131: File Intrusion Detection Monitoring

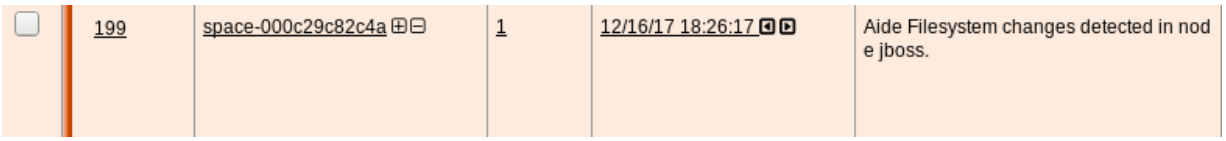


Figure 132 shows the OID details for the trap generated when file or file permission changes are detected in the system.

Figure 132: Trap Details for File Intrusion Detection Monitoring

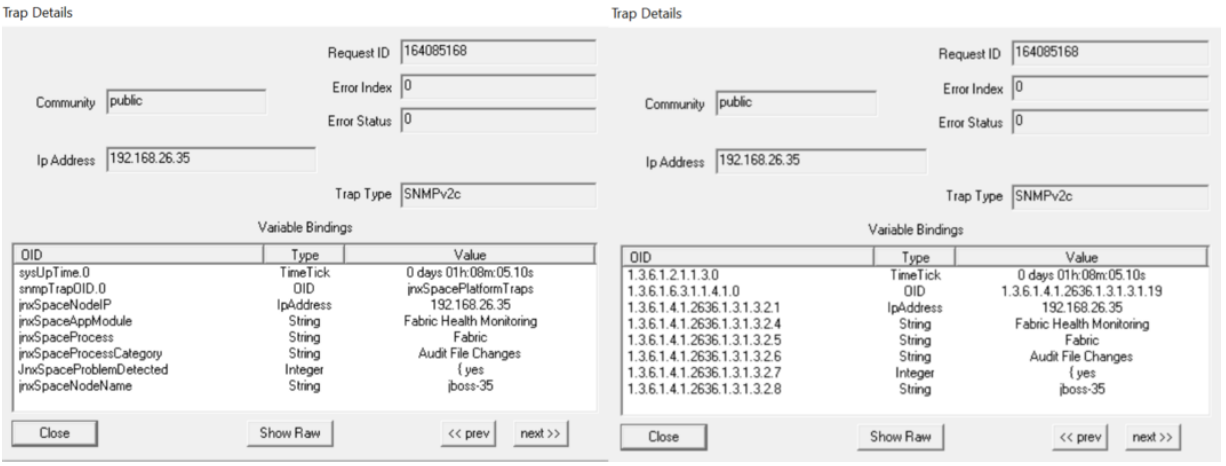


Table 157: SNMP Configuration Parameters: Monitoring Fabric Health *(continued)*

Parameter: Audit Logs Forwarding Failed

When the system fails to forward audit logs to the configured system log server, the trap shown in Figure 133 is generated:

Figure 133: Audit Logs Forwarding Failed

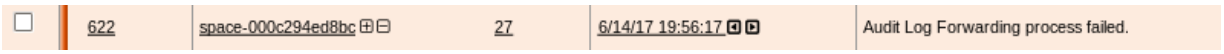


Figure 134 shows the OID details for the trap generated when the system fails to forward audit logs to the configured system log server.

Figure 134: Trap Details When Audit Logs Forwarding Fails

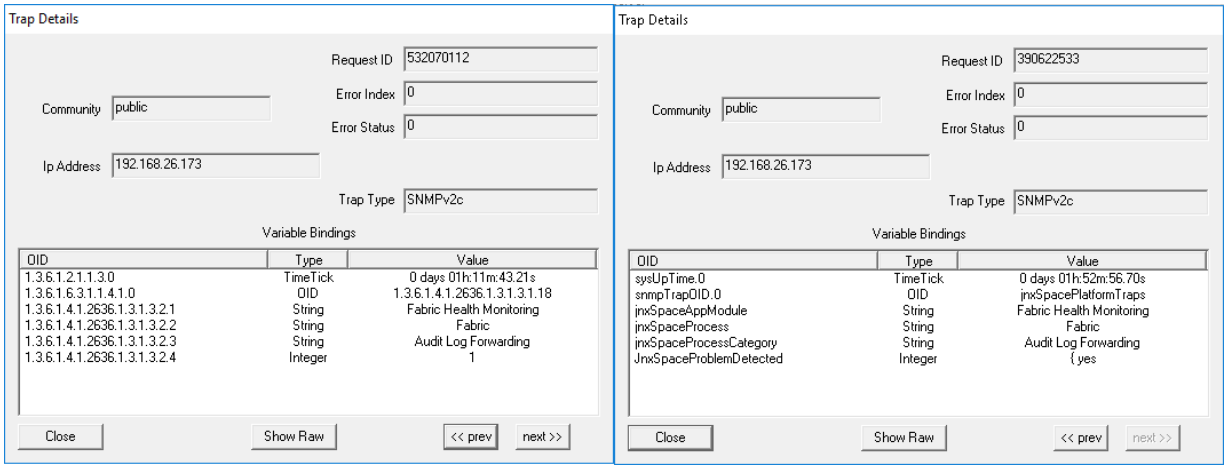


Table 157: SNMP Configuration Parameters: Monitoring Fabric Health *(continued)*

Parameter: One Or More Expected Process Are Inactive

Junos Space monitors critical process like JBoss, MySQL, Apache Web Proxy, OpenNMS and PostgreSQL. If any of these expected processes are inactive, the trap shown in Figure 135 is generated:

Figure 135: One or More Expected Processes Are Inactive

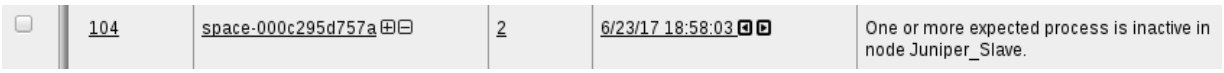


Figure 136 shows the OID details for the trap generated when one or more expected processes are inactive.

Figure 136: Trap Details When One or More Expected Processes Are Inactive

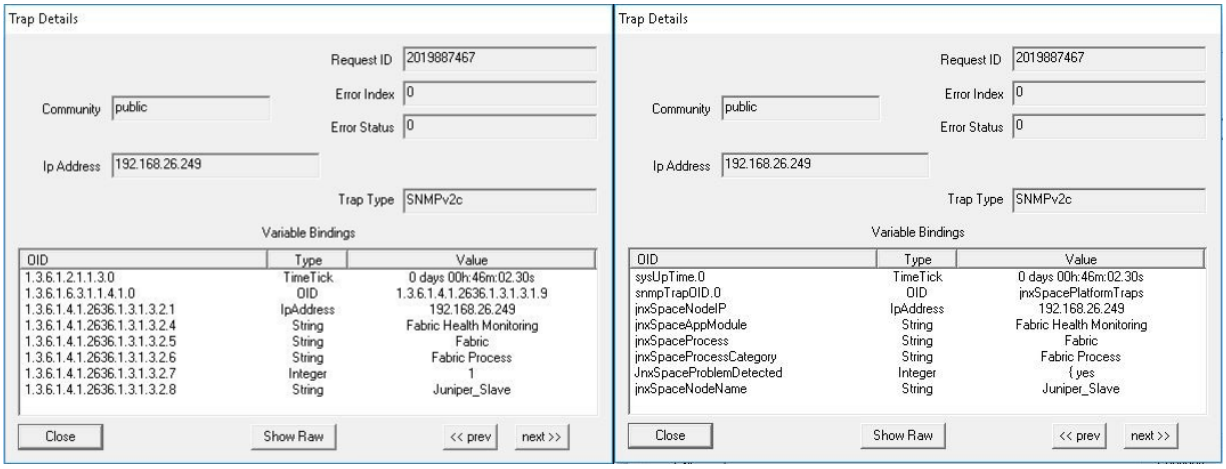


Table 157: SNMP Configuration Parameters: Monitoring Fabric Health *(continued)*

Parameter: One or More Expected Processes Are Inactive On Dedicated FMPM Nodes

When one or more expected processes are inactive on dedicated FMPM nodes, the trap shown in Figure 137 is generated:

Figure 137: One or More Expected Processes Are Inactive On Dedicated FMPM Nodes

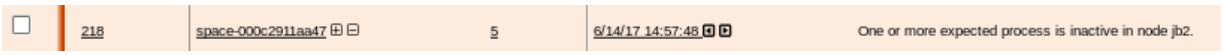
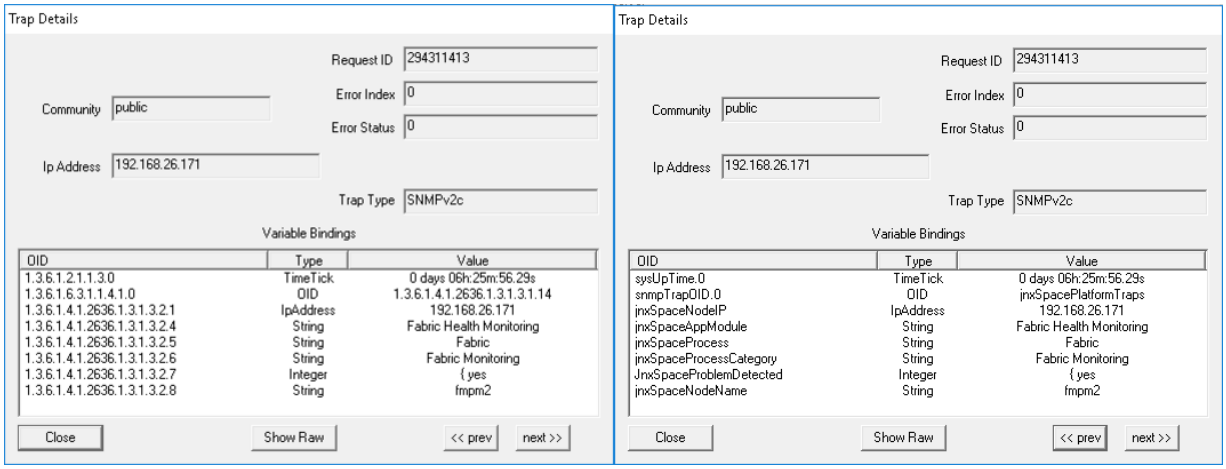


Figure 138 shows the OID details for the trap generated when one or more expected process are inactive on dedicated FMPM nodes.

Figure 138: Trap Details When One or More Expected Processes Are Inactive On Dedicated FMPM Nodes



NOTE: LM-SENSORS-MIB is not supported by the Junos Space virtual appliance, but only by the Junos Space Appliance. Therefore the threshold settings of CPU Max Temp (mC), CPU Min Fan (RPM) and CPU Min Voltage (mV) will not trigger any traps in the virtual appliance.

NOTE: Junos Space supports RAID-related traps on a Junos Space appliance. The following is a sample trap:

```
40948  Normal [+] [-]  2/4/13 09:54:14 [<] [>]  space-node  10.205.56.38
[+] [-]
uei.opennms.org/generic/traps/EnterpriseDefault [+] [-] Edit notifications
 for event
Received unformatted enterprise event (enterprise:.1.3.6.1.4.1.8072.4
generic:6 specific:1001). 1 args: .1.3.6.1.4.1.795.14.1.9000.1="One or
more logical devices contain a bad stripe: controller 1."
```

Starting SNMP Monitoring on Fabric Nodes

To start SNMP monitoring on one or more fabric nodes:

1. Select **Network Management Platform > Administration > Fabric**.

   The Fabric page appears.

2. Select the check box for each fabric node on which you want to start SNMP monitoring.

3. From the Actions menu, select **SNMP Start**.

   The Confirm Start SNMP Agent dialog box is displayed.

4. Click **Yes**.

   Junos Space begins SNMP monitoring on the selected fabric nodes.

   NOTE: This process might take a while.

5. To view the status of SNMP monitoring on the selected fabric nodes, select **Network Monitoring > Node List**.

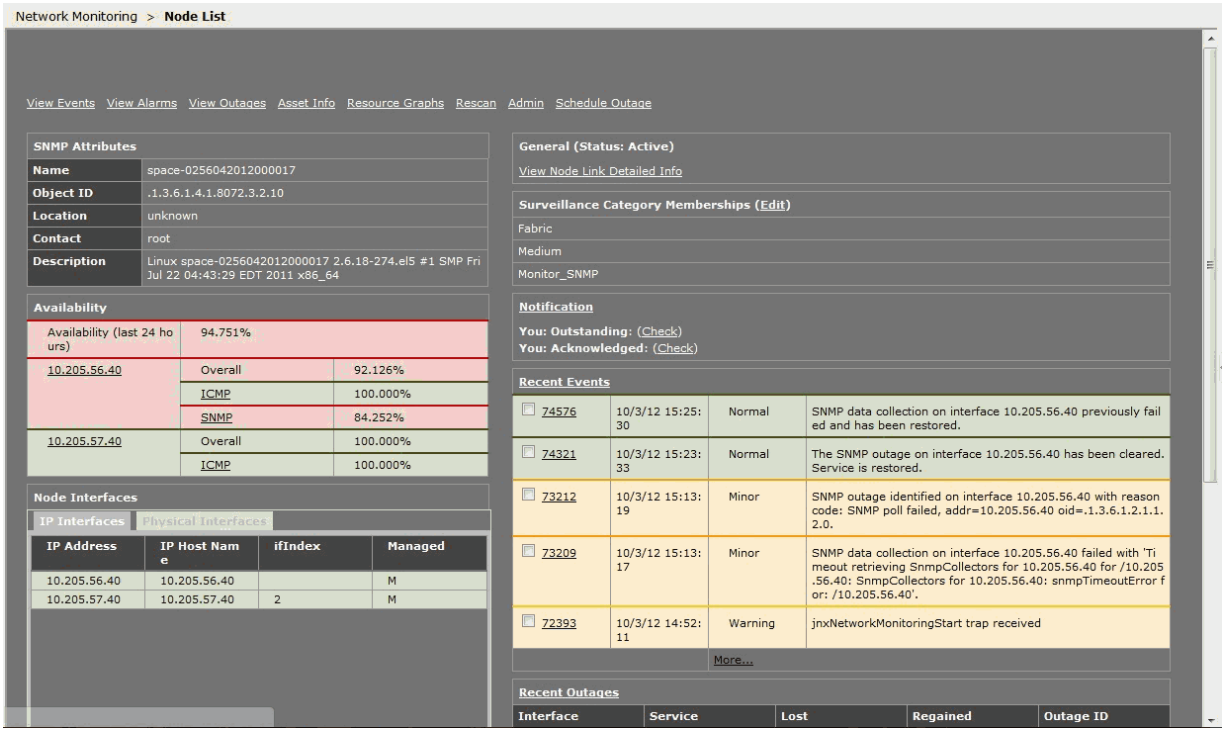
   The Network Monitoring > Node List page appears.

6. Select the node on which you started the SNMP monitoring.

   The Junos Space node is represented as **space-<*number*>**.

Figure 139 shows a sample view of network monitoring details for the selected fabric node.

Figure 139: Network Monitoring Details for the Selected Fabric Node



Under Notification / Recent Events on the right of the Node List page, you see the results of the SNMP monitoring operation.

Stopping SNMP Monitoring on Fabric Nodes

To stop SNMP monitoring on one or more fabric nodes:

1. Select **Network Management Platform > Administration > Fabric**.

   The Fabric page appears.

2. Select the check box for each fabric node on which you want to stop SNMP monitoring.

3. From the Actions menu, select **SNMP Stop**.

   The Confirm Stop SNMP Agent dialog box is displayed.

4. Click **Yes**.

   Junos Space stops SNMP monitoring on the selected fabric nodes.

Restarting SNMP Monitoring on Fabric Nodes

To restart SNMP monitoring on one or more fabric nodes:

1. Select **Network Management Platform > Administration > Fabric**.

   The Fabric page appears.

2. Select the check box for each fabric node on which you want to restart SNMP monitoring.

3. From the Actions menu, select **SNMP Restart**.

   The Confirm Restart SNMP Agent dialog box is displayed.

4. Click **Yes**.

   Junos Space restarts SNMP monitoring on the selected fabric nodes.

Adding a Third-Party SNMP V1 or V2c Manager on a Fabric Node

To add a third-party SNMP V1 or V2c manager on a fabric node:

1. Select **Network Management Platform > Administration > Fabric > SNMP Manager**.

   The SNMP Manager page appears.

2. Click the **Add SNMP Manager** icon.

   The Add 3rd Party SNMP Manager dialog box is displayed.

3. In the **Manager IP** field, enter the SNMP manager IP address.

   NOTE:
   - Depending on whether the Junos Space fabric is configured with only IPv4 addresses or both IPv4 and IPv6 addresses, Junos Space Platform allows you to enter an IPv4 address or either an IPv4 or IPv6 address respectively for the SNMP Manager.
   - The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to http://www.iana.org/assignments/ipv4-address-space for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space for the list of restricted IPv6 addresses.

4. In the **Version** field, select the SNMP version (V1 or V2c) .

5. In the **Community** field, enter the community string.

   Any alphanumeric string (up to 254 characters) is acceptable, including spaces and symbols.

6. Click **OK**.

   The newly added SNMP v1 or v2c Manager is displayed on the SNMP Manager page.

Adding a Third-Party SNMP V3 Manager on a Fabric Node

To add a third-party SNMP V3 manager on a fabric node:

1. Select **Platform > Administration > Fabric > SNMP Manager**.

   The SNMP Manager page appears.

2. Click the **Add** icon.

   The Add 3rd Party SNMP Manager dialog box displays.

3. In the **Manager IP** field, enter the SNMP manager IP address.

   NOTE:
   - Depending on whether the Junos Space fabric is configured with only IPv4 addresses or both IPv4 and IPv6 addresses, Junos Space Platform allows you to enter an IPv4 address or either an IPv4 or IPv6 address respectively for the SNMP Manager.
   - The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to http://www.iana.org/assignments/ipv4-address-space for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space for the list of restricted IPv6 addresses.

4. In the **Version** field, select V3.

5. In the **User Name** field, type the user name.

   The user name can contain a maximum of 32 alphanumeric characters including spaces and symbols.

6. In the **Authentication Type** field, enter the authentication type (**MD5** or **SHA**).

7. In the **Authentication Password** field, enter the authentication password.

   Click the red information icon next to the **Authentication Password** field for information on the password rules.

8. In the **Confirm Authentication password**, enter the authentication password again to confirm the password.

9. From the **Security Level** list, select the security level:
   - **noAuthNoPriv**—Do not specify an authentication or privacy password.
   - **authNoPriv**—Specify only an authentication password.
   - **authPriv**—Specify both authentication and privacy passwords.

10. In the **Privacy Type** field, enter the privacy type (**AES** or **DES**).

11. In the **Privacy Password** field, enter the privacy password.

    Click the red information icon next to the **Authentication Password** field for information on the password rules.

12. In the **Confirm Privacy password** field, enter the privacy password again to confirm the password.

13. Click **OK**.

    The newly added SNMP Manager entry is displayed on the SNMP Manager page.

NOTE: The trap settings for the SNMPv3 manager are not automatically updated in Network Monitoring. Therefore, to ensure that the Network Monitoring receives the traps from Junos Space, you must add the same settings manually in the **/opt/opennms/etc/trapd-configuration.xml** file. Table 158 displays the mapping between the parameters in the **/opt/opennms/etc/trapd-configuration.xml** file and the fields in the Add 3rd Party SNMP Manager page.

The following is a sample configuration in the **/opt/opennms/etc/trapd-configuration.xml** file.

```
<?xml version="1.0"?>
<trapd-configuration snmp-trap-port="162" new-suspect-on-trap="false">
 <snmpv3-user security-name="JunosSpace" auth-passphrase="auth-password"
auth-protocol="MD5"/>
  <snmpv3-user security-name="JunosSpace" auth-passphrase="auth-password"
 auth-protocol="MD5"
      privacy-passphrase="privacy-password" privacy-protocol="DES"/>
</trapd-configuration>
```

Table 158: Mapping of SNMP V3 Settings

Parameter in trapd-configuration.xml File	Field in Add 3rd Party SNMP Manager Page
security-name	**User Name**
auth-passphrase	**Authentication Password**
privacy-passphrase	**Privacy Password**
privacy-protocol	**Privacy Type**

Deleting a Third-Party SNMP Manager from a Fabric Node

To delete a third-party SNMP manager configuration from a fabric node:

1. Select **Platform > Administration > Fabric > SNMP Manager**.

   The SNMP Manager page appears.

2. Select the SNMP manager configuration that you want to remove.

3. Click the **Delete SNMP Manager** icon.

4. To confirm the deletion of the SNMP manager, click **Yes**.

   The deleted SNMP manager is removed from the SNMP Manager page.

Installing StorMan RPM for Monitor RAID Functionality

Download the StorMan RPM package from https://github.com/Juniper/open-media-flow-controller/blob/master/mfc/nokeena/src/base_os/linux_el/el6/arch_x86_64/packages/StorMan-7.31-18856.x86_64.rpm.

To install StorMan RPM:

- From Junos Space Platform CLI, run the following command:

```
# rpm –ivh StorMan-7.31-18856.x86_64.rpm
```

RELATED DOCUMENTATION

Overall System Condition and Fabric Load History Overview | 1159

Fabric Management Overview | 1157
Viewing Nodes in the Fabric | 1186

Viewing Alarms from a Fabric Node

Starting with Junos Space Network Management Platform Release 15.2R1, you can view information about alarms from a fabric node by using the Administration workspace. There are two categories of alarms: acknowledged and outstanding. You must enable the Network Monitoring functionality from the Administration > Applications > Network Management Platform > Manage Services page to view the list of alarms.

> **NOTE:** This task is enabled only for the FMPM node and Junos Space nodes with the SNMP service enabled. You must be assigned appropriate network monitoring privileges to execute this task.

To view information about alarms from a fabric node:

1. On the Junos Space Network Management Platform user interface, select **Administration > Fabric**.

   The Fabric page that appears displays all the nodes in the Junos Space Platform fabric.

2. Right-click a node whose alarm information you need to view and select **View Fabric Node Alarms**.

   The View Fabric Node Alarms page that appears displays the list of outstanding alarms for that node, in a table.

   > **NOTE:** The Alarms(s) outstanding search constraint is applied by default and cannot be removed. You can toggle between the Alarm(s) outstanding constraint and the Alarm(s) acknowledged constraint, which displays the list of acknowledged alarms for the selected node, by clicking the minus (–) icon.

   To know more about the fields displayed in the table, refer to the Viewing Details of an Alarm and Acting on an Alarm section of the "Viewing and Managing Alarms" on page 844 topic.

3. (Optional) To view alarms on all nodes, click the (–) icon corresponding to the node filter in the **Search Constraints** field.

   The View Fabric Node Alarms page displays the list of outstanding or acknowledged alarms for all nodes.

4. You can perform the following tasks on the View Fabric Node Alarms page:

   - Acknowledge, unacknowledge, clear, or escalate one or more alarms, or acknowledge the entire list of outstanding alarms for the selected node. For more information, refer to the Viewing Details of an Alarm and Acting on an Alarm section of the "Viewing and Managing Alarms" on page 844 topic.

   - Toggle between the summary and detailed views of alarms for the selected node:
     - Click the **Long Listing** link at the top of the page for a detailed view.
     - Click the **Short Listing** link at the top of the page for a summary view.

   - View the severity levels for alarms.
     i. Click the **Severity Legend** link at the top of the page.

   For more information about summary and detailed views, and severity levels, refer to the Viewing Alarms in Summary and Detailed Views section of the "Viewing and Managing Alarms" on page 844 topic.

5. Click **Back** (at the top-left corner) to return to the Administration > Fabric page.

Release History Table

Release	Description
15.2R1	Starting with Junos Space Network Management Platform Release 15.2R1, you can view information about alarms from a fabric node by using the Administration workspace.

RELATED DOCUMENTATION

Alarm Notification Configuration Overview | 857

Configuring Alarm Notification | 860

Monitoring Nodes in the Fabric | 1194

Shutting Down or Rebooting Nodes in the Junos Space Fabric

From Junos Space Network Management Platform, the Super Administrator can shut down or reboot fabric nodes when they are moved or when their network settings are reconfigured. You shut down or reboot a fabric node from the Fabric page. Optionally, you can enter a message to display to all users who are logged in to the nodes you choose to shut down or reboot. This message is displayed on the users' CLI consoles and Web browsers.

To shut down or reboot one or more nodes in the fabric:

1. On the Junos Space Network Management Platform UI, select **Administration** > **Fabric**.

   The Fabric page appears.

2. Select the nodes.

3. Select **Shutdown/Reboot Node(s)** from the Actions menu.

   The Shutdown Node dialog box appears.

   > **NOTE:** If the nodes that you selected for shutdown or reboot include hosted virtual machines, then a warning message that the hosted virtual machines will be shut down or rebooted is displayed.

4. Specify, using the **Select action** option button, whether you want to shut down or reboot the node:
   - Select **Shutdown** (which is the default) to shut down the node.
   - Select **Reboot** to reboot the node.
5. (Optional) In the **Shutdown or reboot in minutes** text box, specify the time (in minutes) after which the selected nodes are shut down or rebooted. The default is 1 minute, and the range is 1 through 10 minutes.

6. (Optional) In the **Display message to Console and Browser users** text box, enter a message to notify logged-in users about the reboot or shutdown operation so that users can save any changes.

   The message cannot exceed 500 characters and must contain only letters or numbers. Punctuation marks are not allowed.

   To this message, Junos Space Platform appends a message specifying whether this action is a reboot or shutdown operation and the number of minutes after which the nodes are rebooted or shut down.

> **NOTE:** If you do not enter a message in the **Display message to Console and Browser users** text box, the users will view the following message **The system will be shutdown in X minutes** where X is the value you entered in the **Shutdown or reboot in minutes** text box. If you chose to reboot, users will view **The system will be rebooted in X minutes** where X is the value you entered in the **Shutdown or reboot in minutes** text box.

7. (Optional) In the Reason text box, enter a message to specify the reason for rebooting the node.

   The message cannot exceed 500 characters and can contain letters, numbers, spaces, and special characters. The special characters allowed are hyphen (-), underscore (_), period (.), at symbol (@), dollar ($), caret (^), equal sign (=), square brackets ([]), curly brackets ({}), colon (:), comma (,), and slash (/).

   This message is appended to the audit log entry generated for this task.

8. Click **Confirm** to shut down or reboot the node.

   - If you reboot or shut down one node, the node is shut down or rebooted after the configured time interval.
   - If you shut down multiple nodes, the nodes are shut down after the configured time interval.
   - If you reboot multiple nodes, the nodes are rebooted one by one after the configured time interval in the following sequence with an approximate interval of one minute between the reboot operations:

     a. Node acting as a load balancer

     b. Other nodes

     c. Fault Monitoring and Performance Monitoring (FMPM) node

     d. Node that initiated the reboot operations

   > **NOTE:** If you are shutting down a node after a change of IP address, we recommend that you reboot all nodes for the changes to take effect.

RELATED DOCUMENTATION

Fabric Management Overview | **1157**

Deleting a Node from the Junos Space Fabric | **1259**

Viewing Nodes in the Fabric | **1186**

Disabling the Cassandra Service on a Junos Space Node

You can delete Cassandra nodes from a Junos Space fabric by either deleting the Cassandra nodes or by disabling the Apache Cassandra service on JBoss nodes.

For information about deleting Cassandra nodes from a fabric, see "Deleting a Node from the Junos Space Fabric" on page 1259.

> **NOTE:** When a Cassandra node is deleted, the data stored in the Cassandra node is not moved back to the MySQL database.

To stop and disable the Cassandra service on a JBoss node:

1. On the Junos Space Platform UI, select **Administration > Fabric**.

   The Fabric page appears.

2. Select a Cassandra node that you want to remove from the fabric.

3. Click **Stop Cassandra** to stop the Cassandra service on the node.

   A confirmation dialog box prompts you to confirm that you want to stop the Cassandra service.

   > **NOTE:** Alternatively, you can use the **service cassandra stop** command on the node CLI to stop the Cassandra service.

4. Click **Yes** to stop the Cassandra service on the node.

   The Status dialog box displays the status of the stop the Cassandra service operation.

5. After the Cassandra service is stopped, on the Fabric page, select the node on which you want to disable the Cassandra service.

6. Select **Actions > Disable Cassandra**.

   A confirmation dialog box prompts you to confirm that you want to disable the Cassandra service.

7. Click **Yes** to disable the Cassandra service on the Cassandra node.

   A job is created to disable the Cassandra service on the JBoss node. Navigate to the Job Management page to view job details.

The Cassandra service is disabled on the node and the node acts only as a JBoss node.

RELATED DOCUMENTATION

Starting the Cassandra Service on a Junos Space Node | 1185

Cassandra Nodes in the Junos Space Fabric Overview | 1172

Deleting a Node from the Junos Space Fabric

You can delete a node from the Junos Space fabric directly by selecting the node and selecting **Delete Fabric Node** from the Actions menu. You must remove the deleted node from the network and reimage it. Then, you can add it to the fabric by selecting **Administration** > **Fabric** and the **Add Fabric Node** icon.

NOTE:

- You cannot delete a primary Fault Monitoring and Performance Monitoring (FMPM) node if a secondary FMPM node exists. Junos Space Network Management Platform displays the following error message:
  Primary FMPM node cannot be deleted if secondary FMPM node exist.

  The workaround to delete the primary FMPM node is to perform one of the following actions:

  - Shut down the primary FMPM node and then delete the node.
  - Reboot the primary FMPM node and then delete the node. When you reboot this node, automatic failover takes place and the secondary FMPM node takes over as the primary FMPM node.

- When you delete dedicated database nodes, you cannot delete both the primary and secondary database nodes from the fabric. You can delete either the primary database node or the secondary database node, but not both nodes.

You can delete a node from the fabric under the following conditions:

- In a fabric with two or more nodes, if that node does not disrupt activities of other nodes.
- If a node is configured for high availability—with load balancing and as a database server capability—and another node has the capacity to assume that role. You are prompted to enable that role on another candidate node before deleting that node. If you delete a high-availability node, but no node exists to which you can transfer that role, high availability does not occur.

When you delete a fabric node, Junos Space Platform performs the following tasks:

- Removes references to the host name and IP address of that node from the remaining nodes
- Stops database replication on both the deleted node and the backup database node
- Makes the database backup copy in that node unavailable for the remaining nodes to restore the database from the backup copy
- Copies the database to the new database node
- Shuts down all services that interact with other nodes

When an FMPM node is deleted, the FMPM data from the FMPM node is first backed up and restored on the Junos Space node, and then the FMPM node is deleted from the Junos Space fabric. Thereafter, the network monitoring service is enabled on the Junos Space node.

You can delete only one node at a time. You must have Super Administrator or System Administrative role access privileges to delete a node.

To delete a node:

1. Select **Administration** > **Fabric**.
2. Select the node that you want to delete, and click the **Delete Fabric Node** icon.
3. In the Warning dialog box, confirm that you want to delete the node by clicking **Continue**.
   - If a node you want to delete is not configured for high availability or a node is configured for high availability but there is no other node available to assume that role, the **Delete Node** dialog box appears displaying the node name and management IP address of only the node that you want to delete.
   - If a node is configured for high availability, the **Delete Node** dialog box notifies you of that fact and lists all candidate nodes that have the capacity to assume that role.

     NOTE: When you delete a database node, only non-load-balancer nodes with the same configuration as the node you are deleting are listed as candidate nodes.

   - If a node hosts one or more virtual machines, then the warning message also indicates the IP addresses of the virtual machines that will be deleted.
4. In the **Delete** dialog box, select the node that you want to delete.
5. Click **Delete**.

Node deletion is scheduled as a job immediately after you click **Delete**. Deleting a node generates an audit log entry. The **Delete Fabric Node Job Information** dialog box appears.

6. In the **Delete Fabric Node Job Information** dialog box, click the **Job ID** link.

   The Job Management inventory landing page appears displaying this job. From this page, you can verify and monitor information about the node you are deleting, such as the job type, job ID, percentage of task completion, job state, scheduled start and end times, username, a brief job summary, and so on.

NOTE:

- When you delete a node, a UDP communication exception occurs. This behavior is normal.
- When you delete a load balancer node, a VIP switch may occur and cause the Junos Space Platform progress indicator to appear. This behavior is normal.

RELATED DOCUMENTATION

Fabric Management Overview | **1157**

Viewing Nodes in the Fabric | **1186**

Adding a Node to an Existing Junos Space Fabric | **1176**

Replacing a Failed Junos Space Node | **1272**

Resetting MySQL Replication

From Junos Space Network Management Platform Release 17.2R1 onward, you can reset MySQL replication in runtime. In releases before Junos Space Platform Release 17.2R1, the resetting of MySQL replication is done by backing up and restoring the Junos Space Platform database, which involves backing up the of MySQL database. You can now reset MySQL replication from the Reset MySQL Replication page under the Administration workspace in Junos Space Platform.

Resetting the replication of the MySQL database enables continuous and uninterrupted data replication between the VIP and non-VIP MySQL nodes. This uninterrupted data replication ensures that there is no loss of data or network downtime.

You are alerted on the break in MySQL replication through e-mail notification, an SNMP trap, the **MySQL in out of sync state** parameter in the System Health Report, or the **Database** column on the **Administration > Fabric** page.

To reset MySQL replication in Junos Space Network Management Platform, a user must be a Super Administrator or a System Administrator.

To reset the replication of the MySQL database:

1. On the Junos Space Network Management Platform UI, select **Administration > Fabric**.

   The Fabric page is displayed.

2. Click the **Reset MySQL Replication** button.

   The Reset MySQL Replication page is displayed.

3. To reset the database replication, click the **Reset MySQL Replication** button.

   The Reset MySQL Replication dialog box appears, displaying the job ID corresponding to the reset action.

   a. Click the job ID to view the details of the job.

      You are redirected to the Job Management page with a filtered view of the job corresponding to the reset action.

      Double-click the row corresponding to the job to view details of the job. The View Job Details page displays the details of the job.

   b. Click **OK** to close the page and return to Reset MySQL Replication page.

Failure of the reset job indicates that the database nodes are still not synchronized. You can retry the procedure to reset the replication.

NOTE: Resetting the MySQL replication resets only the replication between database nodes on the active site. If you have configured disaster recovery, we recommend that you back up and restore MySQL database nodes on the standby site as well. To back up and restore MySQL nodes on the standby site, stop and restart the disaster recovery process on Junos Space Network Management Platform.

To stop the backup process at the active site:

1. Log in to the CLI of the Junos Space node at the active site on which the VIP or the eth0:0 interface is configured.

   The Junos Space Settings Menu is displayed.

2. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   You are prompted to enter the administrator password.

3. Enter the administrator password.

4. Type **jmp-dr stop** at the shell prompt and press Enter.

   The disaster recovery process on both sites is stopped.

5. To restart the disaster recovery process on both sites, type **jmp-dr start** and press Enter.

   The disaster recovery process is restarted on both sites.

The MySQL nodes at the standby site are backed up and restored.

RELATED DOCUMENTATION

Viewing Nodes in the Fabric | **1186**

Dedicated Database Nodes in the Junos Space Fabric Overview | **1169**

Shutting Down or Rebooting Nodes in the Junos Space Fabric | **1256**

Modifying the Network Settings of a Node in the Junos Space Fabric

IN THIS SECTION

- Modifying the Fabric Virtual IP Address | **1266**
- Modifying the Network Settings of a Node | **1267**

The Junos Space fabric consists of one or more nodes. Network settings for these nodes enable IP connectivity to external systems as well as internal connectivity between nodes. A Junos Space hardware appliance or a Junos Space virtual appliance is configured as a Junos Space node or a Fault Monitoring and Performance Monitoring (FMPM) node using the Junos Space CLI. You can modify the previously configured settings using the Space Node Settings page.

NOTE: The settings for the hosted virtual machine can also be modified using the Space Node Settings page. For a hosted virtual machine, you can modify the IP address, the subnet mask, and the gateway IP address.

To access the Space Node Settings page, navigate to **Administration** > **Fabric** > **Space Node Settings**. Changing node settings enables you to move the Junos Space fabric from one network location to another location and does not require any reinstallation but only a reboot.

NOTE: Before you modify the network settings, note the following:

- The virtual IP (VIP) address of the Junos Space fabric and the IP address of the Junos Space nodes must be in the same subnet.
- The database VIP address and the node management IP address of the database nodes must be in the same subnet as the VIP address of the fabric.
- The node management IP addresses of all Junos Space nodes in the fabric must be in the same subnet.
- The node management IP addresses of all FMPM nodes in the fabric must be in the same subnet.
- When you modify the device management IP address, all devices that are connected to Junos Space through device-initiated connections must be updated with the new device management IP address by updating the trap target and the **outbound-ssh** configuration with the new device management IP address.
- After you modify the network settings for a node, the node must be rebooted in order for the settings to take effect. Junos Space asks you to confirm the reboot and, upon confirmation, reboots the node and applies the new settings.
- If you modify the settings of a Junos Space node, then all Junos Space nodes in the fabric are rebooted; the FMPM nodes in the fabric are not rebooted. If you modify the settings of an FMPM node, then only the FMPM nodes in the fabric are rebooted; the Junos Space nodes are not rebooted.

This topic includes the following sections:

Modifying the Fabric Virtual IP Address

To modify the virtual IP (VIP) address of the fabric:

> **NOTE:** You can modify the IPv4 VIP address, the IPv6 VIP address, or both.

> **NOTE:** You can modify the database VIP address of dedicated database nodes by selecting the primary database node and modifying the required fields in the **Node Management Interface** section of the Space Node Settings page. See "Modifying the Network Settings of a Node" on page 1267.

1. On the Junos Space Network Management Platform UI, select **Administration** > **Fabric** > **Space Node Settings**.

   The Space Node Settings page is displayed.

2. In the **Fabric Virtual IP** field, modify the IPv4 VIP address of the fabric.

3. In the **Fabric Virtual V6 IP** field, modify the IPv6 VIP address of the fabric.

4. Click **Confirm**.

   The Network Settings Change confirmation dialog box appears.

5. Click **Yes** to save the changes.

   The Reboot Node dialog box appears requesting you to enter a reason for the reboot.

   > **NOTE:** If you do not want to save the changes, click the **No** button on the Network Settings Change confirmation dialog box.

6. Enter the reason for the reboot and click **OK**.

   The nodes are rebooted and the new settings take effect. You can verify that the settings have changed when the nodes are in the **UP** state.

Modifying the Network Settings of a Node

> **NOTE:** Before you modify the network settings of a node, ensure the following:
>
> - For Junos Space nodes, the node management IP address and the VIP address must be in the same subnet.
> - For FMPM nodes, the node management IP address and the FMPM VIP address must be in the same subnet.
> - The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to http://www.iana.org/assignments/ipv4-address-space for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space for the list of restricted IPv6 addresses.
> - All nodes in the Junos Space fabric must have the same type of IP address (or addresses) configured. For example, if a Junos Space node or an FMPM node in a fabric is configured with both IPv4 and IPv6 addresses, then all other Junos Space and FMPM nodes in the fabric must be configured with both IPv4 and IPv6 addresses.

To modify the network settings of a node:

1. On the Junos Space Platform UI, select **Network Management Platform** > **Administration** > **Fabric** > **Space Node Settings**.

   The Space Node Settings page is displayed. The nodes that are part of the fabric are displayed in a table.

2. Click the pencil icon corresponding to the node (or double-click the node) for which you want to modify the settings.

   The network settings for the node are displayed below the row corresponding to the node. The node management interface and device management settings are grouped in the **Node Management Interface** and **Device Management Interface** sections of the Space Node Settings page.

   > **NOTE:** If you have configured the node with only the IPv4 address, you can use this procedure to modify the IPv4 address as well as add an IPv6 address to the node.

3. To modify the node management interface settings:

   a. In the **IP** field, enter the IPv4 address (in dotted-decimal notation) of the node.

   b. In the **Netmask** field, enter the subnet mask (in dotted-decimal notation) for the node.

> **NOTE:** The prefix length range for IPv4 addresses is 1 through 32.

c. In the **Gateway** field, enter the IPv4 address of the default gateway.

d. In the **IPv6** field, enter the IPv6 address of the node.

e. In the **Prefix** field, enter the IPv6 prefix of the node.

> **NOTE:** The prefix length range for IPv6 addresses is 1 through 128.

f. In the **Gateway** field, enter the IPv6 address of the default gateway.

4. To modify the database VIP address:

> **NOTE:** The **databaseVIP** and **databaseV6VIP** fields appear only when you select the primary database node for modifying the network settings.

a. In the **databaseVIP** field, enter the IPv4 VIP address of the database.

b. In the **databaseV6VIP** field, enter the IPv6 VIP address of the database.

5. To modify the device management interface settings:

   a. To enable or disable a separate device management interface:

   - Select **Enable Device Interface** to enable a separate device management interface.

     NOTE:
     - On a Junos Space fabric with two or more Junos Space nodes, if you configure the device management interface on one Junos Space node, then you must also configure the device management interface on all the other Junos Space nodes in that fabric.
     - The device management IP addresses for all Junos Space nodes must be in the same subnet.

   - Clear **Enable Device Interface** to disable a separate device management interface.

     NOTE: If no device management interface is defined, Junos Space Platform uses the node management interface to communicate with devices.

   b. In the **IP** field, enter the IPv4 address (in dotted-decimal notation) of the device management interface.

   c. In the **Netmask** field, enter the subnet mask (in dotted-decimal notation) of the device management interface.

      NOTE: The prefix length range for IPv4 addresses is 1 through 32.

   d. In the **Gateway** field, enter the IPv4 address of the default gateway for the device management interface.

   e. In the **IPv6** field, enter the IPv6 address of the device management interface.

      NOTE: The prefix length range for IPv6 addresses is 1 through 128.

f. In the **Prefix** field, enter the IPv6 prefix of the device management interface.

g. In the **Gateway** field, enter the IPv6 address of the default gateway for the device management interface.

6. Click **OK**.

   Junos Space Platform performs a first-level validation of the modified network settings, which might take a couple of minutes:

   - If there are validation errors, an error message is displayed in a dialog box. Click **OK** to close the dialog box.

     You are taken to the Space Node Settings page. Modify the network settings to ensure that there are no validation errors and repeat this step.

   - If there is no validation error, you are taken to the Space Node Settings page, where the nodes that are part of the fabric are displayed.

7. Click **Confirm** to confirm the settings.

   Junos Space Platform performs a second-level validation of the modified network settings, which might take a couple of minutes:

   - If there are validation errors, an error message is displayed in a dialog box. Click **OK** to close the dialog box.

     You are taken to the Space Node Settings page, where you can modify the network settings to ensure that there are no validation errors and repeat the preceding step.

   - If no validation errors are present, the Network Settings Change confirmation dialog box is displayed.

     a. Click **Yes** to continue.

        The Reboot Node dialog box appears asking you to enter a reason for the reboot.

     b. Enter the reason for the reboot and click **OK**.

        Junos Space Platform sends a message to logged-in users, applies the changed network settings, and reboots the node. After the node is rebooted and is in the **UP** state, the modified network settings can be viewed on the Space Node Settings page.

RELATED DOCUMENTATION

Shutting Down or Rebooting Nodes in the Junos Space Fabric | **1256**

Viewing Nodes in the Fabric | **1186**

Junos Space IPv6 Support Overview | **1152**

Load-Balancing Devices Across Junos Space Nodes

If the devices being managed by Junos Space Network Management Platform are not distributed evenly across Junos Space nodes in the fabric, you can perform load balancing on the Junos Space nodes so that the devices are evenly distributed across each node in the fabric.

To load-balance devices across Junos Space nodes:

1. On the Junos Space Platform user interface, select **Administration** > **Fabric**.

   The Fabric page is displayed with the different nodes in the fabric.

2. Click the **Device Load Balancer** icon on the toolbar.

   The **Device Load Balancer** dialog box appears with the following information displayed for each Junos Space node:

   - Host—Name of the node
   - IP—IP address of the node
   - Status—Status of the node (up or down)
   - Number of devices—Number of devices managed by the node

3. Click **Confirm** to load-balance the devices managed by the Junos Space nodes in the fabric.

   A dialog box is displayed with the job ID.

4. Perform one of the following tasks:

   - Click the job ID hyperlink to go to the Job Management page where you can track the progress of the load balancing.
   - Click **OK** to close the dialog box and return to the Fabric page.

5. (Optional) After the load balancing is completed, click the **Device Load Balancer** icon on the toolbar to view the distribution of devices across nodes in the Device Load Balancer dialog box.

RELATED DOCUMENTATION

Viewing Nodes in the Fabric | **1186**

Monitoring Nodes in the Fabric | **1194**

Replacing a Failed Junos Space Node

This topic provides information about how to replace a failed Junos Space node with a new one. Typically, the status of a failed node is shown as **DOWN** on the Fabric (**Administration** > **Fabric**) page.

To replace a failed Junos Space node:

1. Delete the failed node on the Fabric page by using the **Delete Fabric Node** task. For detailed instructions for deleting a node from a Junos Space cluster, see "Deleting a Node from the Junos Space Fabric" on page 1259.

   When you delete a node, a job is triggered. To confirm whether the node is deleted successfully, check the status of this job on the Job Management page.

2. Depending on whether you are replacing the deleted node with a virtual appliance or a hardware appliance, you can configure deploy the virtual appliance or image the hardware appliance using a USB drive. For more information, refer to the Junos Space virtual appliance or hardware documentation.

3. On the Junos Space Network Management Platform UI, add the node to the existing Junos Space cluster by using the **Administration** > **Fabric** > **Add Fabric Node** task. For detailed instructions about adding a node to a Junos Space cluster, see "Adding a Node to an Existing Junos Space Fabric" on page 1176.

   When you add a node, a job is triggered. To confirm whether the node is added successfully to the existing Junos Space cluster, check the status of this job on the Job Management page. If the job is a success, then the newly added Junos Space node appears on the Fabric page.

RELATED DOCUMENTATION

Fabric Management Overview | **1157**

Overall System Condition and Fabric Load History Overview | **1159**

Generating and Uploading Authentication Keys to Devices

IN THIS SECTION

- Generating Authentication Keys | **1273**
- Uploading Authentication Keys to Multiple Managed Devices for the First Time | **1274**
- Uploading Authentication Keys to Managed Devices With a Key Conflict | **1277**

Junos Space Network Management Platform can authenticate a device either by using credentials (username and password) or by keys. Junos Space Network Management Platform supports RSA, DSA, and ECDSA public-key cryptographic principles to perform key-based authentication. You can select a key size of 2048 or 4096 bits. Junos Space Platform includes a default set of public-private key pairs; the public key is uploaded to the device and the private key is stored on the Junos Space server.

> **NOTE:** If you generated a new set of keys, you can either upload the new keys to the devices or resolve key conflicts when the device is disconnected from Junos Space Platform. For more information about resolving key conflicts, refer to "Resolving Key Conflicts" on page 291.

The following tasks describe how to the generate keys in Junos Space Platform and upload the public keys to the devices:

Generating Authentication Keys

To generate a public/private key pair for authentication during login to network devices:

1. On the Junos Space Network Management Platform user interface, select **Administration > Fabric**.

   The Fabric page is displayed.

2. Click the Manage SSH Key icon on the Actions bar.

   The Key Generator pop-up window is displayed.

3. (Optional) In the **Passphrase** field, enter a passphrase to be used to protect the private key, which remains on the system running Junos Space Network Management Platform and is used during device login. The passphrase must have a minimum of five and a maximum of 40 characters. A long passphrase is harder to break by brute-force guessing. Space, Tab, and Backslash (\) characters are not allowed. Although not mandatory, it is recommended that you set a passphrase to prevent attackers from gaining control of your system and logging in to your managed network devices.

4. (Optional) Select the **Show Passphrase** check box to view the passphrase you entered.

5. From the Algorithm drop down list, select the key algorithm used to the generate the key.

   The options are RSA, DSA, and ECDSA. By default, RSA is selected.

6. From the Key Size drop down list, select the length of the key algorithm that is uploaded to the devices.

   The options are 2048 Bits and 4096 Bits. By default, 2048 Bits is selected.

7. (Optional) Schedule the Junos Space Network Management Platform to generate authentication keys at a later time or immediately.
   - To specify a later start date and time for key generation, select the **Schedule at a later time** check box.
   - To initiate key generation as soon as you click **Generate**, clear the **Schedule at a later time** check box (the default).

   > **NOTE:** The selected time in the scheduler corresponds to the Junos Space server time but uses the local time zone of the client computer.

8. Click **Generate**.

   The Manage SSH Key Job Information dialog box appears, displaying a job ID link for key generation. Click the link to determine whether the key is generated successfully.

> **NOTE:** If there are already scheduled report generation or configuration backup tasks when you change the SSH key, ensure that you update the new SSH Key on the SCP server.

Uploading Authentication Keys to Multiple Managed Devices for the First Time

To upload authentication keys to multiple managed devices for the first time:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Click the Upload Keys to Devices icon on the Actions bar.

   The Upload Keys to Devices pop-up window is displayed.

3. You can upload the keys to one device or multiple devices:

   To upload keys to a single device:

   a. Select the **Add Manually** option button.

      The Authentication Details section that appears displays the options related to manually uploading keys to a single device.

   b. Select the **IP Address** or **Hostname** option button.

      If you selected the IP Address option, enter the IP address of the device.

      > **NOTE:** You can enter the IP address in either IPv4 or IPv6 format.

      If you selected the Hostname option, enter the hostname of the device.

   c. In the **Device Admin** field, enter the appropriate username for that device.

   d. In the **Password** field, enter the password for that device.

   e. (Optional) To authorize a different user on the target device, select the **Authorize different user on device** check box and enter the username in the **User on Device** field.

      If the username you specify in the **User on Device** field does not exist on the device, a user with this username is created and the key is uploaded for this user. If the **User on Device** field is not specified, then the key is uploaded for the device administrator user on the device.

   f. Click **Next**.

      You are directed to the next page. This page displays the details of the device you entered—IP Address/Hostname, Device Admin, Password, and User on Device.

   g. Click **Finish** to upload keys to the device.

      The Job Information dialog box appears.

   h. (Optional) Click the Job ID in the Job Information dialog box to view job details for the upload of keys to the device.

The Job Management page appears. View the job details to know whether this job is successful.

To upload keys to multiple devices:

a. Select **Import From CSV**.

b. (Optional) To see a sample CSV file as a pattern for setting up your own CSV file, select **View Sample CSV**. A separate window appears, allowing you to open or download a sample CSV file.

   Refer to the sample CSV file for the format of entering the device name, IP address, device password, and a username on the device. If the username you specify in the User on Device column does not exist on the device, a user with this username is created and the key is uploaded for this user. If the user on device column is not specified, then the key is uploaded for the device administrator user on the device.

c. When you have a CSV file listing the managed devices and their data, select **Select a CSV To Upload**.

   The Select CSV File dialog box appears.

d. Click **Browse** to navigate to where the CSV file is located on the local file system. Make sure that you select a file that has a .csv extension.

e. Click **Upload** to upload the authentication keys to the device.

   An Information dialog box displays information about the total number of records that are uploaded and whether this operation is a success.

   Junos Space Network Management Platform displays the following error if you try to upload non-CSV file formats:
   Please select a valid CSV file with '.csv' extension.

f. Click **OK** in the information dialog box that appears.

   The green check mark adjacent to the **Select a CSV To Upload** field indicates that the file is successfully uploaded.

g. Click **Next**.

   You are directed to the next page. This page displays the details of the device you entered—IP Address/Hostname, Device Admin, Password, and User on Device.

h. Click **Finish**.

   The Job Information dialog box appears.

i. (Optional) Click the Job ID to view job details for the upload of keys to the device.

The Job Management page appears. View the job details to know whether this job is successful.

New keys generated on Junos Space Platform are automatically uploaded to all managed devices.

Uploading Authentication Keys to Managed Devices With a Key Conflict

To upload authentication keys to one or several managed devices with a key conflict manually:

1. On the Junos Space Network Management Platform user interface, select **Devices > Device Management**.

   The Device Management page is displayed.

2. Select the devices with a key conflict to which you want to upload authentication keys and click the Upload Keys to Devices icon on the Actions bar.

   The Upload Keys to Devices pop-up window is displayed. The IP address fields of the devices are prepopulated.

3. In the **Device Admin** field, enter the appropriate username for that device.

4. In the **Password** field, enter the password for that device.

5. Confirm the password by reentering it in the **Re-enter Password** field.

6. Select **Next** to provide details for the next device.

7. Select **Upload** to upload the authentication keys to the managed devices.
   The Upload Authentication Key dialog box displays a list of devices with their credentials for your verification.

> **NOTE:** If you do not specify a username in the User Name field, the key is uploaded for the "user admin" user on the device. If the username you specify in the User Name field does not exist on the device, a user with this username is created and the key is uploaded for this user.

RELATED DOCUMENTATION

Device Authentication in Junos Space Overview | 281

Device Discovery Profiles Overview | 220

Resolving Key Conflicts | 291

Configuring the ESX or ESXi Server Parameters on a Node in the Junos Space Fabric

If you want to take a snapshot of a Junos Space server running on a virtual machine within an Elastic Sky X (ESX) or Elastic sky X Integrated (ESXi) server, then it is necessary that you provide the ESX or ESXi server information.

To configure the ESX or ESXi server parameters:

1. Select **Administration** > **Fabric**

   The Fabric page appears.

2. Right-click the node that you want to configure and select **ESX Configuration**.

   The ESX Configuration (*Node-IP*) dialog box is displayed, where *Node-IP* is the IP address of the node.

3. In the **Server IP** text box, enter the IP address of the ESX server.

   NOTE:
   - Depending on whether the Junos Space fabric is configured with only IPv4 addresses or both IPv4 and IPv6 addresses, Junos Space Platform allows you to enter an IPv4 address or either an IPv4 or IPv6 address respectively for the ESX server.
   - The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to http://www.iana.org/assignments/ipv4-address-space for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space for the list of restricted IPv6 addresses.

4. In the **VM Name** text box, enter the name of the node as configured on the ESX server.

5. In the **Username** text box, enter the username to log in to the ESX server.

6. In the **Password** field, enter the password to log in to the ESX server.

7. In the **Confirm password** field, reenter the password to log in to the ESX server.

8. Click **Confirm** to save the ESX server configuration.

   The ESX server parameters are saved. You can now proceed with the system snapshot. For more information, see "Creating a System Snapshot" on page 1279.

RELATED DOCUMENTATION

Restoring the System to a Snapshot | 1282

Creating a System Snapshot

You can use the System Snapshot feature to create a snapshot of the system state and roll back the system to a predefined state. The snapshot includes all persistent data on the hard disk including data in the database, system and application configuration files, and application and Linux executables. The System Snapshot is a fabricwide operation that maintains consistency across all nodes in the fabric.

Typically, you use the System Snapshot feature for rolling back the system when it is in an unrecoverable error-state due to corruption of system files, interruption of critical processes, and so on. You can also roll back the system to an older release if the system exhibits undesirable behaviors after a software version upgrade.

> **TIP:** We recommend using System Snapshot before performing significant actions (for example, adding a node to the Junos Space fabric) that have the potential to precipitate the system into an undesirable state. You can delete the snapshot after you have verified that these actions were performed successfully.

System Snapshot is currently supported on a Junos Space fabric that consists of only Junos Space virtual appliances or only Junos Space appliances. This feature is not supported on a hybrid fabric consisting of both Junos Space virtual appliances and Junos Space appliances.

System Snapshot does not impact the performance of a Junos Space virtual appliance. However, if you are using a Junos Space Appliance, performance may be impacted by the number of write operations performed to the snapshot's logical volume.

The maximum size that a snapshot can occupy for Junos Space Network Management Platform is 300 GB. The maximum size that a snapshot can occupy for Junos Space Platform migrated from releases prior to 11.3 is 43 GB. On the Junos Space Appliance, the snapshot becomes invalid if it has been kept for a

long time because usage of the snapshot volume disk space increases as write operations continue. When the usage reaches the maximum size of snapshot volume, the snapshot is disabled. Therefore, ensure that you clear enough hard disk space to accommodate the snapshot.

After executing these commands, start creating the snapshot. The steps used to create a system snapshot for a Junos Space virtual appliance and a Junos Space appliance are almost identical, but there are two additional preliminary steps for the Junos Space virtual appliance:

If you are working with a Junos Space virtual appliance, perform the following steps *before* taking the system snapshot:

> **NOTE:** The following procedure is valid only on a Junos Space virtual appliance deployed on a VMware Elastic Sky X (ESX) or ESXi server.

1. In the Fabric page (**Administration** > **Fabric**), and set the ESX configuration for every node in the fabric. For more information, see "Configuring the ESX or ESXi Server Parameters on a Node in the Junos Space Fabric" on page 1278.

2. Install the VI Toolkit for Perl provided by VMware. For more information, see *Installing VI Toolkit for Perl on Junos Space Virtual Appliance*.

To create a system snapshot:

1. Select **Administration** > **Fabric**

   The Fabric page appears.

2. Click the **System Snapshot** icon.

   The System Snapshot dialog box appears. You can see a system snapshot if you have taken a snapshot earlier. If you are taking the snapshot for the first time, you will not see any snapshots in this dialog box.

   > **NOTE:** If you are creating a system snapshot when a snapshot already exists, the new snapshot will overwrite the older snapshot. Currently, Junos Space Platform can store only one system snapshot.

3. Click **Take Snapshot**.

   The System Snapshot Confirmation dialog box appears.

4. Enter the name of the snapshot in the **Snapshot Name** field.

5. Enter the comments in the **Comment** field.

6. Click **Confirm**.

   A new job is created and the job ID appears in the System Snapshot Job Information dialog box.

7. Click the job ID to view more information about the job created. This action directs you to the Job Management workspace.

   The time taken to complete the snapshot job for a Junos Space virtual appliance is dependent on the number of nodes in the fabric, the disk size of the virtual appliance deployed, the memory size of the virtual appliance, and the performance of the ESX server. The time taken to complete the snapshot job for a Junos Space Appliance is dependent on the disk space used on the appliance.

> **NOTE:** You may not be able to create a snapshot of the system state if any of the following conditions is true:
>
> - There is insufficient disk space on the ESX servers.
> - One of the ESX servers has been incorrectly configured.
> - One of the nodes is down.
> - The fabric consists of both Junos Space virtual appliances and Junos Space appliances.
> - The name specified for the current snapshot is the same as that of the stored snapshot.

RELATED DOCUMENTATION

Deleting a System Snapshot | 1281

Restoring the System to a Snapshot | 1282

Deleting a System Snapshot

To delete a system snapshot:

1. Select **Administration** > **Fabric**. Click the **System Snapshot** icon.

2. Click **Delete**.

   The System Snapshot Deletion dialog box appears. A new job is created and the job ID appears in the System Snapshot Job Information dialog box.

3. Click the job ID to view more information about the job created. This action directs you to the Job Management workspace.

> **NOTE:** You may not be able to delete a snapshot of the system state if any of the following conditions is true:
>
> - One of the ESX servers is incorrectly configured.
> - The fabric consists of both Junos Space VM and Junos Space Appliance.
> - The snapshot does not exist.

RELATED DOCUMENTATION

Creating a System Snapshot | 1279

Restoring the System to a Snapshot | 1282

Restoring the System to a Snapshot

The process to restore a system to a snapshot differs depending on whether you are using a Junos Space VM or a Junos Space Appliance.

To restore a system snapshot when using a Junos Space Virtual Appliance:

1. Select **Administration** > **Fabric**. Click the **System Snapshot** icon.

2. Click **Restore**.

3. Click **OK**.

4. Log in to the ESX servers and power on the virtual machine after a few minutes.

NOTE: If the Junos Space GUI is not accessible on a virtual machine, you can restore the fabric by shutting down every node in the fabric and logging in to ESX servers where the virtual machine is located.

To restore a system snapshot when using a Junos Space Appliance:

1. Select **Administration** > **Fabric**. Click the **System Snapshot** icon.
2. Click **Restore**.

   The System Restore Instruction for Appliance dialog box appears.
3. Follow the instructions on this dialog box.
4. Click **OK**.

NOTE: You may not be able to restore the system to a snapshot if one of the following conditions is true:

- One of the nodes is down.
- New nodes were added after a snapshot was created. A warning message that prompts you to delete the new nodes before restoring is shown.
- Some nodes were deleted after a snapshot was created. A warning message that prompts you to restore the nodes before restoring is shown.

RELATED DOCUMENTATION

Creating a System Snapshot | 1279

Deleting a System Snapshot | 1281

Creating a Unicast Junos Space Cluster

IN THIS SECTION

- Creating a Unicast Junos Space Cluster from a Single Node | 1285
- Creating a Unicast Junos Space Cluster from an Existing Multicast Junos Space Cluster | 1286
- Changing Unicast Communication to Multicast Communication on a Junos Space Cluster | 1287

The nodes of a Junos Space cluster support only multicast traffic. But sometimes, for example, when Internet Group Management Protocol (IGMP) snooping is enabled on switches, unicast communication should be configured on the Junos Space nodes within a subnet so that these nodes can communicate with each other.

Junos Space provides the **changeSettings2staticIP.sh** script to enable you to toggle between unicast and multicast traffic on the nodes of a Junos Space cluster. This script is located in the **/var/www/cgi-bin** folder of a Junos Space node.

Script Syntax

sh changeSettings2StaticIP.sh

Options

- **backup**—Backs up libraries and configuration files from the nodes of the Junos Space cluster
- **restore**—Restores the libraries and configuration files on the nodes of the Junos Space cluster
- **multicast2unicast**—Changes multicast communication to unicast communication on the nodes of a Junos Space cluster
- **unicast2multicast**—Changes unicast communication to multicast communication on the nodes of a Junos Space cluster

When you run the script, the following subsystems in the **domain.xml** configuration file located at **/usr/local/jboss/domain/configuration** are modified:

Table 159: domain.xml Subsystem Parameters Affected When Toggling Between Multicast and Unicast Communication on Junos Space Nodes

Subsystem	Multicast Parameters	Unicast Parameters
mod-cluster	advertise=false, proxy-list	advertise=false, proxy-list
messaging	default-stack=udp, protocol (type=MPING)	default-stack=tcp, protocol (type=TCPPING)

Table 159: domain.xml Subsystem Parameters Affected When Toggling Between Multicast and Unicast Communication on Junos Space Nodes *(continued)*

Subsystem	Multicast Parameters	Unicast Parameters
jgroups	cluster-connections (discovery-group-ref)	connectors (netty-connector), cluster-connections (static-connectors)

You can create a unicast Junos Space cluster from a single node configured for unicast communication or by changing the multicast communication in an existing cluster to unicast communication.

Creating a Unicast Junos Space Cluster from a Single Node

To create a unicast Junos Space cluster from a single node:

1. Create a standalone Junos Space node. For information about creating a standalone Junos Space node, see *Configuring a Junos Space Appliance as a Junos Space Node*.

2. Log in to the CLI of the Junos Space node.

3. On the Junos Space Settings Menu, to access the shell interface:
   - Type **6** if the Junos Space node is a JA2500 Junos Space hardware appliance.
   - Type **7** if the Junos Space node is a virtual appliance.
4. Enter the administrator password.

5. Take a backup of **/usr/local/jboss/domain/configuration/domain.xml** file.

6. Type **cd /var/www/cgi-bin** to navigate to the **cgi-bin** folder.

7. Execute the **changeSettings2StaticIP.sh** script with the **multicast2unicast** option.

   ```
   sh changeSettings2StaticIP.sh multicast2unicast
   ```

8. Restart the jboss-dc process.

   ```
   $/etc/init.d/jboss-dc restart
   ```

9. Restart the jboss process.

```
service jboss restart
```

10. Add a node to form a cluster. For information about adding a node to a cluster, see the "Adding a Node to an Existing Junos Space Fabric" on page 1176.

11. Restart the jboss-dc and jboss processes on all the nodes.

```
$/etc/init.d/jboss-dc restart
```

```
service jboss restart
```

Restart the jboss-dc and jboss processes on all the nodes each time you add a node to the cluster. You can add a maximum of six nodes to a unicast cluster.

Creating a Unicast Junos Space Cluster from an Existing Multicast Junos Space Cluster

To change multicast communication in an existing cluster to unicast communication, you must stop jbosson all nodes and execute the **sh changeSettings2StaticIP.sh** script with the **multicast2unicast** option on the VIP node of the cluster and then restart the jboss-dc and start jboss processes.

To change multicast communication to unicast communication:

1. Log in to the CLI of the Junos Space node on which the VIP or the eth0:0 interface is configured.

2. On the Junos Space Settings Menu, to access the shell interface:
   - Type **6** if the Junos Space node is a JA2500 Junos Space hardware appliance.
   - Type **7** if the Junos Space node is a virtual appliance.
3. Enter the administrator password.

4. Take a backup of **/usr/local/jboss/domain/configuration/domain.xml** file.

5. Type **cd /var/www/cgi-bin** to navigate to the **cgi-bin** folder.

6. Stop the jboss process on all the nodes.

```
services jboss stop
```

7. Execute the **changeSettings2StaticIP.sh** script with the **multicast2unicast** option on the VIP node.

```
sh changeSettings2StaticIP.sh multicast2unicast
```

8. Restart the jboss-dc process on the Junos Space node on which the VIP address is configured.

```
$/etc/init.d/jboss-dc restart
```

9. Start the jboss process on all the nodes.

```
service jboss start
```

10. (Optional) To confirm that the communication is changed from multicast to unicast, execute the **$diff backup/domain.xml /usr/local/jboss/domain/configuration/domain.xml** command on the VIP node to view the differences in the **domain.xml** file before and after executing the **changeSettings2StaticIP.sh** script. See Table 159 for the parameters that change when multicast communication is changed to unicast communication.

Changing Unicast Communication to Multicast Communication on a Junos Space Cluster

To change unicast communication in an existing cluster to multicast communication, you must execute the **sh changeSettings2StaticIP.sh** script with the **unijcast2multicast** option on the VIP node of the cluster and then restart the jboss-dc and jboss processes.

To change unicast communication to multicast communication:

1. Log in to the CLI of the Junos Space node on which the VIP or the eth0:0 interface is configured.
2. On the Junos Space Settings Menu, to access the shell interface:
   - Type **6** if the Junos Space node is a JA2500 Junos Space hardware appliance.
   - Type **7** if the Junos Space node is a virtual appliance.
3. Enter the administrator password.
4. Take a backup of **/usr/local/jboss/domain/configuration/domain.xml** file.
5. Type **cd /var/www/cgi-bin** to navigate to the **cgi-bin** folder.
6. Execute the **changeSettings2StaticIP.sh** script with the **unicast2multicast** option.

```
sh changeSettings2StaticIP.sh unicast2multicast
```

7. Restart the jboss-dc process on the node on which the VIP address is configured.

```
$/etc/init.d/jboss-dc restart
```

8. Restart the jboss process on all the nodes.

```
service jboss restart
```

9. (Optional) To confirm that the communication is changed from unicast to multicast, execute the **$diff backup/domain.xml /usr/local/jboss/domain/configuration/domain.xml** command to view the differences in the **domain.xml** file before and after executing the **changeSettings2StaticIP.sh** script. See Table 159 for the parameters that change when unicast communication is changed to multicast communication.

RELATED DOCUMENTATION

Fabric Management Overview | 1157

NAT Configuration for Junos Space Network Management Platform Overview

IN THIS SECTION

- Using eth0 for Device Management Without a Dedicated Network Monitoring Node | 1290
- Using eth3 for Device Management Without a Dedicated Network Monitoring Node | 1293
- Using eth0 or eth3 for Device Management With a Dedicated Network Monitoring Node | 1296

To manage devices, Junos Space Network Management Platform supports connections initiated by the devices or Junos Space Platform. If a device is managed through a device-initiated connection, Junos Space Platform pushes the device management IP addresses of Junos Space and configures the outbound SSH stanza on the device when the device is discovered or when the device management IP addresses are modified. During device discovery and reconnection to devices, the devices initiate an outbound SSH connection to Junos Space Platform. If a device is managed through a connection initiated by Junos Space, an SSH connection is initiated to the device from Junos Space Platform.

Enabling NAT on your Junos Space setup allows devices placed outside your Junos Space setup to connect to Junos Space Platform and the Junos Space application. Enabling a NAT server on your Junos Space setup uses IP addresses translated through NAT as outbound SSH configuration to connect devices and trap IP addresses translated through NAT to send traps, rather than the actual device management and trap IP addresses. These translated IP addresses are updated and sent to the devices that are managed using a NAT server, after NAT is configured, or when the NAT configuration is updated.

You configure and enable Network Address Translation (NAT) server on a running Junos Space setup from the Administration workspace. You can also configure and enable NAT by using the Junos Space CLI when you create a Junos Space setup during the initial deployment. If you configure a NAT server, you must set a forwarding rule on the NAT server to enable communication between the Junos Space fabric and the devices managed through the NAT server. For more information about enabling NAT when you are configuring the Junos Space Appliance (JA2500) or the Junos Space Virtual Appliance as a Junos Space node or Fault Monitoring and Performance Monitoring (FMPM) node, see one of the following:

- To configure NAT when you are configuring a Junos Space Virtual Appliance, see the Configuring a Junos Space Virtual Appliance as a Junos Space Node, Configuring a Junos Space Virtual Appliance as a Standalone or Primary FMPM Node, and Changing the Network and System Settings of a Junos Space Virtual Appliance topics in the Junos Space Virtual Appliance Installation and Configuration Guide.
- To configure NAT when you are configuring a JA2500 Junos Space Appliance, see the Configuring a Junos Space Appliance as a Junos Space Node, Configuring a Junos Space Appliance as a Standalone or Primary FMPM Node, and Changing Network and System Settings for a Junos Space Appliance topics in the JA2500 Junos Space Appliance Hardware Guide

You can configure the disaster recovery feature and allow database replication in realtime with NAT configuration enabled on your Junos Space setup.

Enabling NAT on a Junos Space setup has the following impact on discovering and managing devices in Junos Space Platform:

- When you configure NAT for the first time, by default, the devices that are managed on Junos Space Platform are not updated with the IP addresses of the Junos Space fabric that are translated through NAT.
- During device discovery, you can choose whether to use the NAT server to route device-initiated connections to Junos Space Platform and manage them through the NAT server. For more information, see “Device Discovery Profiles Overview” on page 220.
- When adding devices using the Model Devices feature, if you choose to use the NAT configuration, the IP addresses of the Junos Space fabric that are translated through NAT are available in the configlet generated from the modeled instance.

- For managed devices routed through a NAT server, Junos Space Platform features such as SSH access to device, Launch WebUI of the devices, and Reactivate an RMA device from the Junos Space UI use the IP addresses of the Junos Space fabric that are translated through NAT.
- Modifying only the NAT address in the network configuration of a Junos Space fabric from the CLI does not trigger a reboot. Junos Space Platform creates a job to update the NAT configuration on all devices managed through the NAT server.

  If you simultaneously modify the NAT configuration and other network settings from the CLI, the NAT configuration changes are discarded and adialog box is displayed with the following message: “Changes to NAT will be discarded as the system required reboot.”

The following sections describe the NAT configuration updated on devices when different interfaces of a Junos Space node are used to deploy the Junos Space fabric :

Using eth0 for Device Management Without a Dedicated Network Monitoring Node

If you use eth0 interface to communicate to devices, the eth0 IP address of each node in the fabric is configured in the outbound SSH configuration on the devices. The virtual IP address (VIP) of the Junos Space setup is set as the trap target to receive SNMP traps from the devices.

Junos Space Platform automatically populates the IP addresses of the Junos Space nodes and the VIP address on the NAT Configuration page. The NAT configuration that is pushed as the outbound SSH connection and the trap target to which the device must send traps are generated as follows:

- If the devices are in your internal network:

  outbound ssh

```
<configuration ...>
            <system>

                <services>

                    <outbound-ssh>

                        <client>

                            <name>cluster_CLUSTERNAME</name>

                            <device-id>9A1E0</device-id>

      ...
                            <services>netconf</services>

                            <servers>
```

```
                                <name>$NODE1_ETH0_IP</name>

                                <port>7804</port>

                            </servers>

                            <servers>

                                <name>$NODE2_ETH0_IP</name>

                                <port>7804</port>

                            </servers>
                            ...

                        </client>

                    </outbound-ssh>

                </services>

            </system>

 </configuration>
```

trap target

```
<configuration>
  <snmp>
    <v3>
      <target-address>
        <name>TA_SPACE</name>
        <address>$SPACE_ETH0_VIP</address>
      </target-address>
    </v3>
  </snmp>
</configuration>
```

- If the devices are in your external (to the NAT server) network:

outbound ssh

```
<configuration ...>
            <system>

                <services>

                    <outbound-ssh>

                        <client>

                            <name>cluster_CLUSTERNAME</name>

                            <device-id>E9A1E0</device-id>

      ...
                            <services>netconf</services>

                            <servers>

                                <name>$NODE1_NAT_SSH_IP</name>

                                <port>$NODE1_NAT_SSH_PORT</port>

                            </servers>

                            <servers>

                                <name>$NODE2_NAT_SSH_IP</name>

                                <port>$NODE2_NAT_SSH_PORT</port>

                            </servers>
                            ...
                        </client>

                    </outbound-ssh>

                </services>

            </system>

</configuration>
```

trap target

```
<configuration>
  <snmp>
    <v3>
      <target-address>
         <name>TA_SPACE</name>
        <address>$SPACE_NAT_VIP</address>
        <port>$SPACE_NAT_TRAP_PORT</port>
      </target-address>
    </v3>
  </snmp>
</configuration
```

A NAT server should be configured with a rule to forward device-initiated connections destined to **$NODEx_NAT_SSH_IP** and **$NODEx_NAT_SSH_PORT** to **$NODEx_ETH0_IP:7804**. Similarly, traps destined to **$SPACE_NAT_VIP** and **$SPACE_NAT_TRAP_PORT** must be forwarded to **$SPACE_ETH0_VIP:162**.

Using eth3 for Device Management Without a Dedicated Network Monitoring Node

If you use eth3 interface to communicate to devices, the eth3 IP address of each node in the fabric is configured in the outbound SSH configuration on the devices. The eth3 IP address of the active node (that currently works as a Network Monitoring node) is set as the trap target to receive SNMP traps from the devices.

Junos Space Platform automatically populates the IP addresses of the Junos Space nodes and the address of the network monitoring node on the NAT Configuration page. The NAT configuration that is pushed as the outbound SSH connection and the trap target to which the device must send traps are generated as follows:

- If the devices are in your internal network:

outbound ssh

```
<configuration ...>
            <system>

                <services>

                    <outbound-ssh>

                        <client>
```

```
                            <name>cluster_CLUSTERNAME</name>

                            <device-id>9A1E0</device-id>

      ...
                            <services>netconf</services>

                            <servers>

                                <name>$NODE1_ETH3_IP</name>

                                <port>7804</port>

                            </servers>

                            <servers>

                                <name>$NODE2_ETH3_IP</name>

                                <port>7804</port>

                            </servers>
                            ...

                        </client>

                    </outbound-ssh>

                </services>

            </system>

 </configuration>
```

trap target

```
<configuration>
  <snmp>
    <v3>
      <target-address>
        <name>TA_SPACE</name>
        <address>$NODE      _ETH3_IP</address>
                    opennms
      </target-address>
    </v3>
```

```
  </snmp>
</configuration>
```

- If the devices are in your external (to the NAT server) network:

  outbound ssh

```
<configuration ...>
            <system>

                <services>

                    <outbound-ssh>

                        <client>

                            <name>cluster_CLUSTERNAME</name>

                            <device-id>E9A1E0</device-id>

      ...
                            <services>netconf</services>

                            <servers>

                                <name>$NODE1_NAT_SSH_IP</name>

                                <port>$NODE1_NAT_SSH_PORT</port>

                            </servers>

                            <servers>

                                <name>$NODE2_NAT_SSH_IP</name>

                                <port>$NODE2_NAT_SSH_PORT</port>

                            </servers>
                            ...
                        </client>

                    </outbound-ssh>

                </services>
```

```
            </system>

</configuration>
```

trap target

```
<configuration>
  <snmp>
    <v3>
      <target-address>
         <name>TA_SPACE</name>
        <address>$NODE_opennms_NAT_TRAP_IP</address>
        <port>$NODE_opennms_NAT_TRAP_PORT</port>
      </target-address>
    </v3>
  </snmp>
</configuration
```

A NAT server should be configured with a rule to forward device-initiated connections destined to **$NODEx_NAT_SSH_IP** and **$NODEx_NAT_SSH_PORT**, to **$NODEx_ETH3_IP:7804**. Similarly, traps destined to **$NODE$_{opennms}$_NAT_TRAP_IP** and **$NODE$_{opennms}$_NAT_TRAP_PORT** must be forwarded to **$NODE$_{opennms}$_ETH3_IP:162**.

Using eth0 or eth3 for Device Management With a Dedicated Network Monitoring Node

If you use eth3 interface to communicate to devices, the eth3 IP address of each node is configured in the outbound SSH configuration on the devices. Similarly, if you use eth0 interface to communicate to devices, the eth0 IP address of each node is configured in the outbound SSH configuration on the devices. The VIP address of the dedicated Network Monitoring node is configured as the trap target to send SNMP traps from the devices.

Junos Space Platform automatically populates the IP addresses of the Junos Space nodes and the VIP address on the NAT Configuration page. The NAT configuration that is pushed as the outbound SSH connection and the trap target to which the device must send traps are generated as follows:

- If the devices are in your internal network:

outbound ssh

```
<configuration ...>
            <system>
```

```
                <services>
                    <outbound-ssh>
                        <client>
                            <name>cluster_CLUSTERNAME</name>
                            <device-id>9A1E0</device-id>
     ...
                            <services>netconf</services>
                            <servers>
                                <name>$NODE1_ETH0_IP</name>
                                <port>7804</port>
                            </servers>
                            <servers>
                                <name>$NODE2_ETH0_IP</name>
                                <port>7804</port>
                            </servers>
                            ...
                        </client>
                    </outbound-ssh>
                </services>
            </system>
</configuration>
```

trap target

```
<configuration>
  <snmp>
    <v3>
      <target-address>
        <name>TA_SPACE</name>
        <address>$OPENNMSNODE_ETH0_VIP</address>
      </target-address>
    </v3>
  </snmp>
</configuration>
```

- If the devices are in your external (to the NAT server) network:

outbound ssh

```
<configuration ...>
            <system>

                <services>

                    <outbound-ssh>

                        <client>

                            <name>cluster_CLUSTERNAME</name>

                            <device-id>E9A1E0</device-id>

      ...
                            <services>netconf</services>

                            <servers>

                                <name>$NODE1_NAT_SSH_IP</name>

                                <port>$NODE1_NAT_SSH_PORT</port>

                            </servers>

                            <servers>

                                <name>$NODE2_NAT_SSH_IP</name>
```

```
                                <port>$NODE2_NAT_SSH_PORT</port>

                            </servers>
                            ...
                        </client>

                    </outbound-ssh>

                </services>

            </system>

 </configuration>
```

trap target

```
<configuration>
  <snmp>
    <v3>
      <target-address>
         <name>TA_SPACE</name>
        <address>$OPENNMSNODE_NAT_VIP</address>
        <port>$OPENNMSNODE_NAT_TRAP_PORT</port>
      </target-address>
    </v3>
  </snmp>
</configuration
```

A NAT server should be configured with a rule to forward device-initiated connections destined to **$NODEx_NAT_SSH_IP** and **$NODEx_NAT_SSH_PORT**, to **$NODEx_ETH0_IP:7804**. Similarly, traps destined to **$OPENNMSNODE_NAT_VIP** and **$OPENNMSNODE_NAT_TRAP_PORT** must be forwarded to **$OPENNMSNODE_ETH0_VIP:162**.

Release History Table

Release	Description
16.1R1	Enabling NAT on your Junos Space setup allows devices placed outside your Junos Space setup to connect to Junos Space Platform and the Junos Space application.

RELATED DOCUMENTATION

Configuring the NAT IP Addresses and Ports on Junos Space Platform | 1300
Modifying the NAT IP Addresses and Ports on Junos Space Platform | 1302
Disabling the NAT Configuration on Junos Space Platform | 1303

Configuring the NAT IP Addresses and Ports on Junos Space Platform

You configure a NAT server on your Junos Space setup when you want to route connections through a NAT server. Configuring a NAT server updates the device management IP addresses that devices use to connect to Junos Space Platform from Junos Space fabric IP addresses to IP addresses translated through NAT. For more information about the impact of using a NAT server and the IP addresses pushed to the outbound stanza of devices, see "NAT Configuration for Junos Space Network Management Platform Overview" on page 1288.

To configure and enable NAT IP addresses and NAT ports:

1. On the Junos Space Platform UI, select **Administration > Fabric > NAT Configuration**.

   The NAT Configuration page appears.

2. To enable NAT configuration on the Junos Space setup, select the **Enable NAT** check box.

   The fields to enter the NAT IP addresses and ports are displayed. Table 160 displays the columns on the NAT Configuration page. By default, the fields to enter the NAT IP addresses and ports for nodes in the Junos Space fabric are dimmed.

   The number of rows displayed in the NAT Configuration page depend on the number of nodes and how you have configured the Junos Space fabric.

   Table 160: Columns on the NAT Configuration Page

Column	Description
Node Name	Name of the node as configured in the Junos Space fabric
Node IPV4	IPv4 address of the node
Node IPV6	IPv6 address of the node
Service	Type of service - Outbound-SSH or trap
NAT IPV4	IPv4 address used to route connections to a specific node
NAT IPV6	IPv6 address used to route connections to a specific node

Table 160: Columns on the NAT Configuration Page *(continued)*

Column	Description
NAT IPV4 Port	Port used to route IPv4 connections to a specific node
NAT IPV6 Port	Port used to route IPv6 connections to a specific node

3. Click the NAT IPV4 column corresponding to the node for which you need to enter the IP address of the NAT server.

   The corresponding cell in the NATIPV4 column is displayed.

4. Enter the IP address in the cell.

5. Click the NAT PortV4 column corresponding to the node for which you need to enter the port number of the NAT server.

   The corresponding cell in the NAT PortV4 column is displayed.

6. Enter the port number in the cell.

7. Repeat steps 3 through 6 to enter the IP addresses and port numbers for all nodes in the Junos Space fabric.

8. Click **Save** to save the NAT configuration.

   An Information dialog box is displayed with the following message: **NAT Configuration updated successfully. but there is no external device to update NAT configuration**.

   Click **OK** to close the Information dialog box.

   A job is triggered to update the NAT configuration on all devices that use the NAT server to route connections to Junos Space Platform.

To discard the NAT configuration you entered, click **Cancel**.

You are redirected to the Fabric page.

RELATED DOCUMENTATION

NAT Configuration for Junos Space Network Management Platform Overview | **1288**

Modifying the NAT IP Addresses and Ports on Junos Space Platform | **1302**

Modifying the NAT IP Addresses and Ports on Junos Space Platform

You modify the NAT configuration on Junos Space Platform when you need different NAT addresses or ports to route connections to Junos Space Platform. Modifying the NAT configuration updates the IP addresses that devices use to connect to Junos Space Platform to IP addresses of the Junos Space fabric that are translated through NAT.

To modify the NAT IP addresses and NAT ports:

1. On the Junos Space Platform UI, select **Administration > Fabric > NAT Configuration**.

   The NAT Configuration page appears.

2. To modify the NAT configuration on the Junos Space setup:

   a. (Optional) Click the NAT IPV4 column corresponding to the node for which you need to enter the IP address of the NAT server.

      The corresponding cell in the NATIPV4 column is displayed.

   b. (Optional) Enter a different IP address in the cell.

   c. (Optional) Click the NAT PortV4 column corresponding to the node for which you need to enter the port number of the NAT server.

      The corresponding cell in the NAT PortV4 column is displayed.

   d. (Optional) Enter a different port number in the cell.

   e. Repeat steps 3 through 6 to enter the IP addresses and port numbers for nodes in the Junos Space fabric.

3. Click **Save** to save the NAT configuration.

   a. If all the devices currently managed by Junos Space Platform are in the internal network, an Information dialog box is displayed with the following message: **NAT Configuration updated successfully. but there is no external device to update NAT configuration**

      Click **OK** to close the Information dialog box.

      You are redirected to the Fabric page.

b. If some of the devices are currently managed by Junos Space Platform are outside the internal network, the updated NAT configuration is pushed to the outbound ssh stanza of the these devices.

A job is triggered to update the NAT configuration on all devices that use the NAT server to route connections to Junos Space Platform.

To discard the modifications to NAT configuration, click **Cancel**.

You are redirected to the Fabric page.

RELATED DOCUMENTATION

NAT Configuration for Junos Space Network Management Platform Overview | 1288

Configuring the NAT IP Addresses and Ports on Junos Space Platform | 1300

Disabling the NAT Configuration on Junos Space Platform | 1303

Disabling the NAT Configuration on Junos Space Platform

You disable the NAT configuration when you no longer have devices outside the Junos Space setup connecting to Junos Space Platform.

To disable the NAT configuration:

1. On the Junos Space Platform UI, select **Administration > Fabric > NAT Configuration**.

   The NAT Configuration page appears.

2. To disable NAT configuration on the Junos Space setup, clear the **Enable NAT** check box.

3. Click **Save** to save the modifications to NAT configuration and **Cancel** to discard the modifications..

   The NAT configuration is disabled. You are redirected to the Fabric page.

To retain the NAT configuration, click **Cancel**.

You are redirected to the Fabric page.

RELATED DOCUMENTATION

NAT Configuration for Junos Space Network Management Platform Overview | 1288

CHAPTER 70

Backing up and Restoring the Junos Space Platform Database

IN THIS CHAPTER

- Backing Up and Restoring the Database Overview | **1305**
- Backing Up the Junos Space Network Management Platform Database | **1308**
- Restoring the Junos Space Network Management Platform Database | **1314**
- Deleting Junos Space Network Management Platform Database Backup Files | **1319**
- Viewing Database Backup Files | **1320**

Backing Up and Restoring the Database Overview

As System Administrator, you can perform Junos Space Network Management Platform database backup, restore, and delete operations. Junos Space Network Management Platform enables you to back up the complete system data, which includes the MySQL database, the Cassandra database, and the network-monitoring database (containing the PostgreSQL data, configuration files, and performance data files). Because of this feature, if a system crashes, you can add a new system (Return Material Authorization (RMA)) and restore the configuration that existed in the crashed system from the backup file.

To perform database backup or restore operations, you must be assigned the System Administrator role. Only a System Administrator can initiate a backup operation from the Administration > Database Backup and Restore workspace.

When you initiate a backup operation, all databases are backed up by default. Because the network-monitoring database could be fairly large in size, you can select whether or not to back up this database from the Junos Space GUI by clearing the Network Monitoring check box from the Database Backup page (Administration > Database Backup and Restore > Database Backup). If sufficient disk space is unavailable, Junos Space Network Management Platform throws an error. Duration of the backup job might vary depending on the database size.

> **NOTE:** Junos Space Network Management Platform allows you to perform backup and restore operations even when the network-monitoring service is turned off.

If you have the Cassandra service running on at least one node in the fabric, the Cassandra database is backed up by default. If you do not want the Cassandra database to be backed up, you can clear the Cassandra check box from the Database Backup page (Administration > Database Backup and Restore > Database Backup).

In Junos Space Release 13.1 and earlier, a local backup operation saves the backup file of the Junos Space database to a specific folder (**/var/cache/jboss/backup**) on the active node. As an administrator, you may want the backup files to exist on both the primary and secondary nodes so that when one of the nodes crashes you can restore the system from the backup file saved on the other node. In this release, backup is initiated on the secondary node and the backup file is saved to the default location (**/var/cache/jboss/backup**) on the secondary node. If the backup operation is successful, then the backup file is synchronized with (copied to) the primary node. The following are the advantages:

- The backup file is present on both the primary and secondary nodes due to which you can restore the system if one of the nodes crashes or is corrupted.
- System performance of the primary node is not impacted because the backup operation is initiated on the secondary node.

NOTE:

- When dedicated database nodes are present in the Junos Space fabric, database backup files are always stored in the dedicated database nodes. The database backups created before dedicated database nodes are added remain in the old nodes; the old backups are not moved to the dedicated database nodes. You can restore the system configuration from the old backup files even when later backups are present in the dedicated database nodes.
- For disaster recovery, different additional database backup and restoration provisions must be made.

Restore the Junos Space Network Management Platform database if any of the following issues occur:

- Junos Space Network Management Platform data is corrupted and you need to replace it with uncorrupted data.
- The Junos Space Network Management Platform software is corrupted and you reinstalled the Junos Space Network Management Platform software.
- You can restore a Junos Space database from a backup that is taken in the same release version only. For example, you can restore a Junos Space Release *xx* database only from a backup that is taken in Junos Space Release *xx*, where *xx* represents the version number.

In a multinode setup, the same backup file can exist on both the primary and secondary nodes. In such cases, when you choose to restore a system from a local backup file, Junos Space Network Management Platform randomly chooses a backup file from one of the nodes to restore the system.

Backing Up a Database

By default, Junos Space Network Management Platform automatically backs up the database once a week. However, the administrator can schedule a backup to run at anytime and perform either local or remote backup operations. All jobs that are completed before the start of the backup operation are captured in the database backup file.

During a backup operation, Junos Space Network Management Platform archives data files and the logical logs that record database transactions, such as the users, nodes, devices, and added or deleted services in Junos Space Network Management Platform.

The administrator can perform a local or remote database backup operation. When the administrator performs a local backup operation, Junos Space Network Management Platform backs up all database data and log files to a local default directory **/var/cache/jboss/backup**. You cannot specify a different database backup file location for a local backup. No such restriction exists when backing up to a remote location.

For a remote backup, use only a Linux-based server. You must specify a remote host that is configured to run the Linux Secure Copy Protocol (SCP) command. You must also specify a valid user ID and password

for the remote host. To ensure that you are using a valid directory, check the destination directory before you initiate a database backup operation to the remote system.

For instructions on how to back up the Junos Space Network Management Platform database, see "Backing Up the Junos Space Network Management Platform Database" on page 1308.

Restoring a Database

When the System Administrator performs a restore database operation, data from a previous database backup is used to restore the Junos Space Network Management Platform database to its previous state. The administrator can restore the database through the Administration > Database Backup and Restore workspace (see "Restoring the Junos Space Network Management Platform Database" on page 1314).

The restore database operation is performed while Junos Space Network Management Platform is in maintenance-mode. The system is therefore down on all nodes in the fabric and only the Web proxy is running. During this time, all Junos Space users, except the maintenance-mode administrator, are locked out of the Junos Space Network Management Platform.

> **NOTE:** After the Junos Space Network Management Platform database is restored, the Security Design database must be manually reindexed. For more information about Security Design, see the Security Design documentation.

RELATED DOCUMENTATION

- Restoring the Junos Space Network Management Platform Database | **1314**
- Backing Up the Junos Space Network Management Platform Database | **1308**
- Maintenance Mode Overview | **1153**

Backing Up the Junos Space Network Management Platform Database

A user with the System Administrator or Super Administrator role can back up the Junos Space Platform database and later use the backup file to restore the Junos Space Platform database to a previous state. You can back up all system data, which includes all databases (MySQL, Cassandra, and network monitoring data), DMI schemas, and configuration files, and save the backup file on both the primary and secondary nodes. This fallback system allows you to restore the system even if one of the database nodes crashes. Typically, the database backup file contains configuration data for managed nodes, managed devices, deployed services, scheduled jobs, Junos Space Platform users, network monitoring, and so on.

You can perform local and remote backup and restore operations. A local backup operation copies the backup file to the default directory **/var/cache/jboss/backup**. A remote backup operation copies the backup file to remote network hosts.

NOTE: When you perform a local backup operation:

- On a fabric with one node, the backup file is saved on the primary node.
- On a fabric with multiple nodes, only the primary and secondary nodes are considered database nodes and therefore contain database backup files. The backup operation is initiated only from the secondary node and the backup file is saved to the **/var/cache/jboss/backup** location on the secondary node.

  If the backup operation is successful, then the backup file is synchronized with (copied to) the primary node and both primary and secondary nodes have the same backup file. However, if the backup operation fails on the secondary node (for reasons such as insufficient space), then the backup operation is performed on the primary node.
- If dedicated database nodes are present in the fabric, the backup files are always stored in the dedicated database nodes.
- In a fabric with dedicated database nodes, the MySQL database backup is initiated on the secondary database node and the backup file is saved to the **/var/cache/jboss/backup** directory on the secondary database node.

  If the backup operation is successful, then the backup file is synchronized with (copied to) the primary database node and both the primary and secondary database nodes have the same backup file.
- If Cassandra nodes are present in the fabric, the Cassandra database from one of the Cassandra nodes is backed up.
- The network monitoring data backup is initiated on the Junos Space node when no FMPM node exists. When FMPM nodes are present in the fabric, the network monitoring data backup is initiated on the FMPM node and then copied to the database nodes and stored.

When you back up the Junos Space Platform database, an audit log entry is automatically generated. From the Audit Log inventory page, you can filter the data by using the **Database Backup** keyword to view details about the database backup operations that were performed.

To back up the Junos Space Platform database:

1. On the Junos Space Platform user interface, select **Administration** > **Database Backup and Restore**.

   The Database Backup and Restore page appears.

2. Click the **Database Backup** icon.

The Database Backup page appears. The default behavior is a backup operation that occurs once a week (see 7 for more information).

3. You can back up the database file locally on a fabric node or to a remote location (by using the Secure Copy Protocol [SCP]):

   - To back up the file locally, retain the selection of **local** in the **Mode** field (in the **Mode Options** section). In the local mode, the Junos Space Platform database backup is stored to the default directory **/var/cache/jboss/backup**.

     NOTE: When the local mode option is selected, the **Username**, **Password**, **Confirm password**, **Machine IP**, and **Directory** fields on the Database Backup page are disabled.

   - To back up the file remotely, do the following:

     a. In the **Mode** field (in the **Mode Options** section), select **remote**.

     b. In the **Username** field, enter a username to access the remote host server.

     c. In the **Password** field, enter the corresponding password.

     d. In the **Confirm password** field, reenter the password.

     e. In the **Machine IP** field, enter the remote host server IP address.

        NOTE:
        - Depending on whether the Junos Space fabric is configured with only IPv4 addresses or both IPv4 and IPv6 addresses, Junos Space Platform allows you to enter an IPv4 address or either an IPv4 or IPv6 address respectively for the SCP server.
        - The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to http://www.iana.org/assignments/ipv4-address-space for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space for the list of restricted IPv6 addresses.

     f. In the **Directory** field, enter a directory path on the remote host server where you want to store the database backup file.

        NOTE: The directory path must already exist on the remote host server.

4. In the **Content Options** section, do one of the following:

   - Retain the selection of the **Network Monitoring** check box for Junos Space Platform to back up network monitoring data, in addition to the Cassandra database (if the option is selected) and the default MySQL data.

     If you choose to back up network monitoring data, then the following information is backed up:

     - PostgreSQL network monitoring database
     - Configuration files in the **/opt/opennms/etc** directory and its subdirectories
     - Graph data in the **/var/opennms/rrd** directory and its subdirectories

   - Clear the **Network Monitoring** check box if you do not want to back up network monitoring data.
   - Retain selection of the **Cassandra** check box for Junos Space Platform to back up files in the Cassandra database, in addition to the network monitoring data (if the option is selected) and the default MySQL data.
   - Clear the **Cassandra** check box if you do not want to back up the Cassandra database.

     The Cassandra check box is available only if the Cassandra service is running on at least one node in the fabric. The check box is selected by default; you can clear the selection if you do not want to back up the Cassandra database files.
   - Select the **DMI Schemas** check box if you want to include the DMI schemas in the backup. This check box is available only from Release 17.2R1 onward.

     > **NOTE:** By default, MySQL data is always backed up; the **MySQL** check box is selected and disabled.

5. (Optional) In the **Comment** field, add a comment to describe or otherwise identify the backup operation.

6. (Optional) Specify whether the Junos Space Platform database backup operation should occur immediately or be scheduled for later:

   - Select the **Schedule at a later time** check box to specify a later start date and time for the database backup operation.
   - Clear the **Schedule at a later time** check box (the default) to initiate the database backup operation as soon as you click **Backup**.

     > **NOTE:** The selected time in the scheduler corresponds to the Junos Space server time but uses the local time zone of the client computer.

7. (Optional) Specify whether the database backup should recur or not:
   - To schedule a recurring backup:

     NOTE: The **Repeat** check box is selected by default and the default behavior is a backup operation that occurs once a week.

     a. Specify the database backup recurrence by setting the interval and the increment, as indicated in Table 161. The default recurrence interval is 1 hour.

     Table 161: Backup Schedule Units and Increments

Interval	Increment
Minutes	Specify the number of minutes after which the backup should recur.
Hourly	Specify the number of hours after which the backup should recur.
Daily	Specify the number of days after which the backup should recur.
Weekly	Specify the number of weeks after which the backup should recur. In addition, specify the *additional* days of the week on which the backup should recur by selecting the appropriate check box. The day on which you specified the recurrence is already selected and disabled.
Monthly	Specify the number of months after which the backup should recur. In addition, specify whether the backup should recur on the same date of the month (the default) or the same day of the specific week of the month. For example, if you configure the monthly recurrence on July 8 2015, which is the second Wednesday in July, you can specify whether the backup should recur on the 8th of the month or on the second Wednesday of the month.
Yearly	Specify the number of years after which the backup should recur. In addition, specify whether the backup should recur on the same date of the year (the default) or the same day of the specific week of the month every year. For example, if you configure the yearly recurrence on July 8 2015, which is the second Wednesday in July, you can specify whether the backup should recur on 8th July or on the second Wednesday of July.

     b. Specify when the recurrence should end in the **Ends on** field.
        - To specify that the recurrence does not end (the default), select **Never**.

    - To specify a date and time by which the recurrence ends, select the option button and specify a date and time

  - To specify that the database backup does not recur, clear the **Repeat** check box.

8. Click **Backup**.

   A confirmation dialog box appears, which displays:
   Warning: Taking database backup may have an impact on system performance. Do you want to continue?

9. Click **OK** on the confirmation dialog box to back up the Junos Space database.

   The **Backup Job Information** dialog box appears. Perform one of the following actions:

   - Click the Job ID on this dialog box to view the database backup job details on the Job Management page.
   - If you do not wish to view the job details (that is, whether the database backup job is a success or a failure), click **OK** on this dialog box. You are returned to the Database Backup and Restore page. If the backup job is successful, the new backup file is displayed on this page.
   - Click **Cancel** on this dialog box to cancel the database backup operation.

All the backup files are saved in a single compressed TAR file (extension **.tgz**) with the filename **backup_*timestamp*.tgz**, where *timestamp* indicates the date and time when the backup was performed. The backup file contains either MySQL, Cassandra, and network monitoring data, MySQL and network monitoring data, MySQL and Cassandra data, or just MySQL data depending on whether you have chosen to back up the Cassandra and network monitoring data or not.

For troubleshooting, see the following logs on the Junos Space server:

- **/var/log/nma.log**
- **/var/log/nma/*.log**
- **/tmp/maintenance.log**

RELATED DOCUMENTATION

Restoring the Junos Space Network Management Platform Database | **1314**

Viewing Database Backup Files | **1320**

Deleting Junos Space Network Management Platform Database Backup Files | **1319**

Backing Up and Restoring the Database Overview | **1305**

Viewing Audit Logs | **1117**

Viewing Jobs | **972**

Restoring the Junos Space Network Management Platform Database

IN THIS SECTION

- Restoring the Junos Space Platform Database from a Local Backup File | 1315
- Restoring the Junos Space Platform Database from a Remote Backup File | 1316

You can restore any archived Junos Space Network Management Platform database to restore your Junos Space system to a previous state. When you initiate a restore database operation, Junos Space Platform is shut down on all nodes in the fabric and the system goes into maintenance mode, during which time only one maintenance mode administrator can log in to the system at a time. After the restore database operation is completed, Junos Space Platform is restarted and users can access the Junos Space UI.

Because you can back up the Junos Space database locally (that is, in the Junos Space server) or remotely (in another system), both the database backup files are displayed in the Junos Space GUI. You can restore the Junos Space database from the local or remote database backup file.

To restore a Junos Space Platform database, you must have System Administrator privileges and be a Maintenance Mode administrator.

NOTE:

- Before you restore a Junos Space Platform database, wait until all jobs that are currently running are completed.
- Junos Space Platform supports only the standard U.S. English on the remote server and does not support any other local languages.

To view information about the available database backup files before you select a Junos Space Platform database to restore, see “Viewing Database Backup Files” on page 1320.

CAUTION: The restore operation replaces the existing data with the contents of the backup file. Merging of data does not occur.

Restoring the Junos Space Platform Database from a Local Backup File

To restore the Junos Space Platform database to a previous state:

1. Select **Administration** > **Database Backup and Restore**.

   The Database Backup and Restore page appears, displaying the previous database backups.

2. Select the database backup file you want to restore.

   NOTE: In a multinode setup, the selected backup file may exist on both the primary and secondary nodes. The **Machine** column on the Database Backup and Restore page reflects the IP addresses of these nodes where the backup file is stored. In such cases where the same backup file exists on more than one node, Junos Space selects a backup file from one of the nodes randomly for the restore operation.

3. Select **Restore** from the Actions menu.

   The Restore confirmation dialog box appears and displays the following message:

   Warning: you are about to enter maintenance mode. Space will be shutdown to restore database. All data generated after the selected backup will be lost, and other users will not be able to access the system during the operation. Do you want to continue?

   CAUTION: This confirmation dialog box must display the name of the backup file that you selected for the restore operation. If not, wait for a few seconds until the backup filename appears before you proceed to the next step. Otherwise, the restore operation may fail.

4. Click **Continue** in the Restore confirmation dialog box.

   Junos Space Platform prompts you to enter a username and password to enter maintenance mode.

5. Enter the maintenance mode username and password.

6. Click **OK**.

   Junos Space Platform is shut down and other users will be unable to access the system during the restore database operation.

   The Restore Database Status dialog box displays the status for the restore database operation.

7. In the Restore Database Status dialog box, click **Return to Maintenance Menu**.

   The Maintenance Mode Options page appears.

8. In the Maintenance Mode Actions dialog box, click **Log Out and Exit Maintenance Mode**. This action exits maintenance mode, starts up Junos Space Platform, and returns to normal operational mode.

   The process of exiting maintenance mode and restarting Junos Space Platform takes several minutes.

   NOTE: During startup, the startup page first displays a message indicating that Junos Space Platform is starting up and then displays a progress bar indicating the percentage of startup completed, the estimated time left for the Junos Space Platform to start, and a list of tasks to complete (with an indication of the current task being carried out). When a task is successfully completed, a message is displayed; if a task fails, an error message is displayed indicating why the task failed.

Depending on the contents of the backup file (which might contain either MySQL, Cassandra, and network monitoring data, MySQL and network monitoring data, MySQL and Cassandra data, or just MySQL data), data is refreshed on the system.

Restoring the Junos Space Platform Database from a Remote Backup File

You need to restore the Junos Space Platform database from a remote file if the Junos Space system to which you are restoring it has been reimaged.

The restore operation restores the data based on the contents of the backup file. The backup file can contain both network monitoring and MySQL data, or just MySQL data.

CAUTION:

- The database restoration operation is performed while Junos Space Platform is in maintenance mode. During this time, all Junos Space Platform users, except the maintenance mode administrator, are locked out of the Junos Space system.

To restore a database, you must have System Administrator privileges and be a Maintenance Mode administrator.

To restore the database from a remote file:

1. On the Junos Space Platform user interface, select **Administration > Database Backup and Restore**.

   The Database Backup and Restore page appears.

2. Click the **Restore From Remote File** icon.

   The Restore From Remote File page appears.

3. In the **Username** field, enter a username to access the remote server.

4. In the **Password** field, enter the corresponding password.

5. In the **Confirm password** field, reenter the password.

6. In the **Machine IP** field, enter the IP address of the remote server on which the backup file is located.

   NOTE:
   - Depending on whether the Junos Space fabric is configured with only IPv4 addresses or both IPv4 and IPv6 addresses, Junos Space Platform allows you to enter an IPv4 address or either an IPv4 or IPv6 address respectively for the SCP server.
   - The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to http://www.iana.org/assignments/ipv4-address-space for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space for the list of restricted IPv6 addresses.

7. In the **File Path** field, enter enter the full path of the backup file stored on the remote server.

8. (Optional) In the **Comment** field, enter a comment to capture any information about this database restore operation.

9. Click **Restore** to start the restore database operation.

   The Restore Database confirmation dialog box appears.

   WARNING: You must log in to Junos Space Maintenance mode. Junos Space Platform shuts down to restore the database. All data generated after the selected backup will be lost. Junos Space users will not be able to log in to Junos Space Platform during the restore database operation.

10. Click **Continue** in the Restore Database dialog box.

    Junos Space Platform prompts you to enter a username and password to log in to the Maintenance mode.

11. Enter the maintenance mode username and password.

12. Click **OK**.

    Junos Space Platform is shut down and other users will be unable to access the system during the restore database operation.

    The Restore Database Status dialog box displays the status of the restore database operation.

13. In the Restore Database Status dialog box, click **Return to Maintenance Menu**.

    The Maintenance Mode Options page appears.

14. In the Maintenance Mode Options page, click **Log Out and Exit Maintenance Mode**. This action exits maintenance mode, starts up Junos Space Platform, and returns to normal operational mode.

    The process of exiting maintenance mode and restarting Junos Space Platform takes several minutes.

    > **NOTE:** During startup, the startup page first displays a message indicating that Junos Space Platform is starting up and then displays a progress bar indicating the percentage of startup completed, the estimated time left for the Junos Space Platform to start, and a list of tasks to complete (with an indication of the current task being carried out). When a task is successfully completed, a message is displayed; if a task fails, an error message is displayed indicating why the task failed.

Depending on the contents of the backup file (which might contain either MySQL, Cassandra, and network monitoring data, MySQL and network monitoring data, MySQL and Cassandra data, or just MySQL data), data is refreshed on the system.

RELATED DOCUMENTATION

- Backing Up the Junos Space Network Management Platform Database | 1308
- Viewing Database Backup Files | 1320
- Deleting Junos Space Network Management Platform Database Backup Files | 1319
- Maintenance Mode Overview | 1153

Deleting Junos Space Network Management Platform Database Backup Files

The System Administrator can delete archived database backup files that are no longer useful for restore operations.

NOTE:

- From Junos Space Network Management Platform Release 15.1R1 onward, Junos Space Platform provides a built-in purging policy that enables you purge database backup files automatically based on a specified disk usage threshold or at regularly scheduled intervals. For more information, see "Junos Space Purging Policy and Purging Categories Overview" on page 1566.
- When you delete a database backup file from the Database Backup and Restore inventory page, the backup file is permanently deleted from Junos Space Platform and cannot be retrieved or restored.
- In a multinode setup, the selected backup file may exist on both the primary and secondary nodes. The **Machine** column on the Database Backup and Restore page reflects the IP addresses of these nodes where the backup file is stored. In such cases where the same backup file exists on more than one node, when you delete a backup file, the backup file is deleted from both the nodes.

To delete a Junos Space Platform database backup file:

1. On the Junos Space Platform UI, select **Administration > Database Backup and Restore**.

   The Database Backup and Restore page appears.

2. From the Database Backup and Restore page tabular view, select one or more database backup files that you want to delete.

3. (Optional) View the database backup file detailed information before deleting the file. Detailed database backup file information appears as columns in the table.

4. Click the **Delete Backup** icon on the toolbar.

   Junos Space Platform deletes the selected Junos Space Platform database backup files. The deleted backup files are no longer displayed on the inventory page and are deleted from the **/var/cache/jboss/backup** directory if it is a local backup operation or from the remote location for a remote backup operation.

CAUTION: When you delete a local backup file, if the backup file is present on both the primary and secondary nodes, then this file is deleted from both the nodes.

When you delete a database backup file, an audit log entry is automatically generated and details about the deleted file is recorded.

To obtain details about the backup files that were deleted from an audit log entry:

1. On the Junos Space Platform user interface, select **Audit Logs** > **Audit Log**.

   The Audit Log inventory page appears, displaying all log entries in a table.

2. Filter data in the **Task** column by using the **Delete Backup** keyword.

   The Audit Log page displays only the audit log entries that were generated when the database backup files were deleted.

3. Double-click an audit log entry.

   The Audit Log Detail page appears. On this page, the **Affected Objects** section displays the list of database backup files that were deleted and the **Affected Object Detail** section displays details about each database backup file.

4. Click **OK** on the Audit Log Detail page to exit this page.

   You are returned to the Audit Log page.

RELATED DOCUMENTATION

Backing Up the Junos Space Network Management Platform Database | 1308

Restoring the Junos Space Network Management Platform Database | 1314

Viewing Database Backup Files | 1320

Viewing Database Backup Files

The Database Backup and Restore inventory page displays information about Junos Space Network Management Platform database backups, including the date and time of the backup operation, the backup file name and location, and the IP address of the Junos Space Appliance that is backed up. From the

Database Backup and Restore inventory page, the administrator can restore a database or delete a database backup.

- Changing Views | 1321
- Viewing Database Details | 1321
- Managing Database Commands | 1322

Changing Views

You can view database backup information in tabular view. Each database backup is represented by a row in the table.

To change views:

1. On the Junos Space Network Management Platform user interface, select **Administration** > **Database Backup and Restore**.

   The Database Backup and Restore page appears.

2. Click the **Display Quick View** icon on the Database Backup and Restore page title bar.

Viewing Database Details

To view detailed database backup information:

1. On the Junos Space Network Management Platform user interface, select **Administration** > **Database Backup and Restore**.

   The Database Backup and Restore page appears.

2. Double-click a database in tabular view. The View Backup page appears.

   Table 162 defines the database backup detailed information.

   Table 162: Fields in the Manage Databases Table

Field	Description
Name	Name of the database backup file. Junos Space Network Management Platform automatically assigns a name to the backup file.
Backup Date	Date and time of the database backup operation
Comment	Information a Junos Space user optionally provides in the Comments field of the Backup page when scheduling a database backup operation

Table 162: Fields in the Manage Databases Table *(continued)*

Machine	IP address of the Junos Space Appliance on which the database backup operation is performed. In a multinode setup, the backup operation is initiated on the secondary node. When the backup operation is successfully completed, the backup file is synchronized with (copied to) the primary node. In such scenarios, the backup file exists on both the primary and secondary nodes, and the IP addresses of both the nodes are displayed in the **Machine** field.
File Path	File path for the database backup. For a local backup operation, this column displays the default directory location where the backup file is stored, which is: **/var/cache/jboss/backup**. For a remote backup operation, this column displays the path to the backup file on the remote server.

Managing Database Commands

From the Database Backup and Restore page, you can perform the following actions:

- Delete Database Backup—"Deleting Junos Space Network Management Platform Database Backup Files" on page 1319
- Restore Database—"Restoring the Junos Space Network Management Platform Database" on page 1314
- Tag It—"Tagging an Object" on page 1526
- View Tags—"Tagging an Object" on page 1526
- Clear All Selections—Clears all selections you made on the Database Backup and Restore page.

RELATED DOCUMENTATION

Deleting Junos Space Network Management Platform Database Backup Files | **1319**

Restoring the Junos Space Network Management Platform Database | **1314**

Backing Up the Junos Space Network Management Platform Database | **1308**

Tagging an Object | **1526**

CHAPTER 71

Managing Licenses

IN THIS CHAPTER

- Generating and Uploading the Junos Space License Key File | 1323
- Viewing Junos Space Licenses | 1326

Generating and Uploading the Junos Space License Key File

IN THIS SECTION

- Generating the Junos Space License Key File | 1325
- Uploading the Junos Space License Key File Contents | 1325

NOTE:

- From Junos Space Network Management Platform Release 13.1R1 onward, the licensing model of Junos Space does not require license keys for Junos Space applications. Nevertheless, a license file is still needed for the Junos Space Platform functionality because the default Junos Space Platform license file is valid only for 60 days after which the Junos Space Platform functionality is not available.

  When you purchase a commercial version of Junos Space Platform, Juniper Networks provides you with a license file that does not have any expiry date. After you import this license into Junos Space Platform, you have access to the full Junos Space Platform functionality for an unlimited period.

- Since Junos Space applications do not use license keys, the Licenses page (**Administration** > **Licenses**) does not display licensing information for any Junos Space applications that you might have purchased and installed. However, if you use Junos Space Platform with only Service Now and Service Insight installed, licensing information for those applications is displayed on the Licenses page. To find out the licensing information about Junos Space applications that you purchased, contact the Juniper Technical Assistance Center.

The Junos Space Platform software provides a default, 60-day trial license. After 60 days, the use of the Junos Space Platform software expires except for the **Import License** action. The administrator must activate the software with the Juniper Networks license key to regain use of the Junos Space Platform. Two weeks before the license expiration date, a license expiration warning appears when users log in to Junos Space Platform.

Junos Space Platform license management involves a two-step process:

1. Generating the license key file. Juniper Networks uses a license management system (LMS) to manage the deployment of the Junos Space Platform product—appliances, connection points, connections, and applications. When you order Junos Space Platform, the Juniper Networks LMS sends you an e-mail with an authorization code and a software serial number and instructions on how to generate a license key.

2. Import the license key into Junos Space Platform. The system administrator must import the Junos Space license key file from the Licenses page (**Administration** > **Licenses**) to use Junos Space Platform beyond the trial period.

This topic includes the following sections:

Generating the Junos Space License Key File

When you order Junos Space Platform, Juniper Networks sends an e-mail containing an authorization code and a software serial number (the serial number that identifies the software installation) along with instructions on how to generate the license key.

When you order a Junos Space Appliance, Juniper Networks sends an e-mail containing the serial number for the appliance that is licensed for the appropriate stock-keeping unit (SKU).

Uploading the Junos Space License Key File Contents

To upload the Junos Space license key file, perform the following steps:

1. Open the Juniper Networks Authorization Codes e-mail you received and follow the directions.

2. Open the Junos Space license key text file attached to the e-mail and copy all the contents.

3. In the Junos Space Platform UI, select **Administration** > **Licenses**.

   The Licenses page appears.

4. Click the **Import License** icon.

   The Import License page appears.

5. Paste the contents of the Junos Space license key text file in the **License data** field.

   Follow the below example of a license key:

```
Juniper Networks Junos Space License File (v1)
For Junos Space Platform
Generated on 2013-11-18T17:28:53Z
This license file is for the deployment using:
Serial Number: 90211111111111
This license file enables the following:
Junos Space Network Management Platform per core(Qty: 1)
This license file reflects the following SKUs:
JS-PLATFORM
-----SIGNATURE-----
PJ6RbY2b92+UzXHwx3jTn7kkojkZxJvbVdHtq5RNDrB1nLuTgKNG42KuAU7RBc3eK40Jb9BZYH1m
  aI3SN/9CSPI3+FK1h095RXG7GMMfcu3Q7nlBJUcJytTVZGlWkm6n8o8Wj2ymei58pFLf9TMHYY2J
  OqTqWHJNAKJ2/tlxacGJ1yFtyJGWz4KbSiXAawiHtk9hfi2v0vzA+3ByyZ8PZSIpsIBk5m3Pqtr+
  2/pxkNGXoCsEnhRAoPticSVibzsoMCo/Myzymp3KaqWHwe/PpPkwL28+I1AB6NA/FUxxTlgjp2k1
  YJZt9rSsJATDgH3lcU1zqSVuGn2DNNhX5F3xTw==
```

> **NOTE:** Paste the license data into the **License data** field using Ctrl+V or by selecting paste in the browser Edit menu.

6. Click **Upload**.

   The license key data is uploaded to the Junos Space Platform database. A message indicating that the Junos Space license is uploaded successfully appears.

7. Click **OK**.

   The Junos Space license appears on the Licenses inventory page.

RELATED DOCUMENTATION

Viewing Junos Space Licenses | 1326

Viewing Junos Space Licenses

> **NOTE:** From Junos Space Network Management Platform Release 13.1R1 onward, the licensing model of Junos Space does not require license keys for Junos Space applications. However, a license file is still needed for the Junos Space Platform functionality because the default Junos Space Platform license file is valid only for 60 days after which the Junos Space Platform functionality is not available.
>
> Since Junos Space applications do not use license keys, the Licenses page (**Administration** > **Licenses**) does not display licensing information for any Junos Space applications that you might have purchased and installed. However, if you use Junos Space Platform with only Service Now and Service Insight installed, licensing information for those applications is displayed on the Licenses page. To find out the licensing information about Junos Space applications that you purchased, please contact the Juniper Technical Assistance Center.

The Licenses inventory page displays the Junos Space Platform license that the administrator has uploaded. For more information about obtaining and uploading the Junos Space Platform license, see "Generating and Uploading the Junos Space License Key File" on page 1323.

The Licenses page displays the Junos Space Platform trial license until you upload the one specifically generated for your software installation.

To view the Junos Space license details:

1. In the Junos Space Platform UI, select **Administration** > **Licenses**.

   The Licenses page appears displaying the details of the Junos Space Platform license, as shown in Table 163.

Table 163: License Details

Field	Description
License Type	The Junos Space Platform license can either be a trial license installed (**Trial**) with the Junos Space Platform software image or a commercial one (**Commerical**) that you upload into Junos Space Platform.
Sku Model #	The Junos Space Platform license stock-keeping unit (SKU) model number. If the license is a trial license, the SKU displayed is **Trial-license**. If it is a commercial license, the license SKU is displayed; for example, **JS-PLATFORM**.
Total License Days	For a trial license, the total number of license days is 60. For a commercial license, the total number of license days is unlimited (**Unlimited**).
Remaining License Days	For a trial license, the remaining number of days is the countdown of the number of days since you installed Junos Space Platform (for example, 36). For a commercial license, the remaining number of days is unlimited (**Unlimited**).

RELATED DOCUMENTATION

Exporting the License Inventory | 312

CHAPTER 72

Managing Junos Space Platform and Applications

IN THIS CHAPTER

- Managing Junos Space Applications Overview | **1328**
- Upgrading Junos Space Network Management Platform Overview | **1330**
- Junos Space Store Overview | **1333**
- Configuring and Managing Junos Space Store | **1334**
- Running Applications in Separate Server Instances | **1338**
- Managing Junos Space Applications | **1343**
- Modifying Settings of Junos Space Applications | **1345**
- Modifying Junos Space Network Management Platform Settings | **1346**
- Managing File Integrity Check | **1367**
- Starting, Stopping, and Restarting Services | **1369**
- Adding a Junos Space Application | **1372**
- Upgrading a Junos Space Application | **1376**
- Upgrading Junos Space Network Management Platform | **1378**
- Synchronizing Time Across Junos Space Nodes | **1384**
- Upgrading to Junos Space Network Management Platform Release 16.1R1 | **1387**
- Uninstalling a Junos Space Application | **1406**

Managing Junos Space Applications Overview

You can use the Applications page to manage Junos Space Network Management Platform and all other separately packaged applications.

In this page you can perform the following tasks:

- Install a new Junos Space application by using the **Administration** > **Applications** > **Add Application** task (see "Adding a Junos Space Application" on page 1372).
- Upgrade Junos Space Platform by using the **Administration** > **Applications** > **Upgrade Platform** action (see "Upgrading Junos Space Network Management Platform" on page 1378). Junos Space Network

Management Platform provides the running environment for all Junos Space applications, so upgrading it interrupts the operation.

- Upgrade a Junos Space application while Junos Space Platform is still running by using the **Administration** > **Applications** > **Upgrade Application** action (see "Upgrading a Junos Space Application" on page 1376).
- Uninstall a Junos Space application while Junos Space Platform is still running by using the **Administration** > **Applications** > **Uninstall Application** action (see "Uninstalling a Junos Space Application" on page 1406).
- Modify application settings by using the **Administration** > **Applications** > **Modify Application Settings** action (see "Modifying Settings of Junos Space Applications" on page 1345).
- Start, stop, or restart services by using the **Administration** > **Applications** > **Manage Services** action (see "Starting, Stopping, and Restarting Services" on page 933).
- Tag applications to categorize them for filtering and performing Manage Applications actions by using the **Administration** > **Applications** > **Tag It** action (see "Tagging an Object" on page 1526).
- View tags that you have already created on a selected application by using the **Administration** > **Applications** > **View Tags** action (see "Viewing Tags for a Managed Object" on page 1532).

> **NOTE:** The Junos Space Platform image file contains only the files pertaining to Junos Space Network Management Platform. Junos Space applications are packaged in separate image files. To install or upgrade an application, the administrator must download the application image file from the Juniper Networks support site (https://www.juniper.net/support/products/space/#sw), upload the application image file to Junos Space Platform, and install or upgrade the application. When the application is installed, you can launch it from Application Chooser. When you upgrade Junos Space Network Management Platform, all applications are disabled; you can upgrade the disabled applications after upgrading Junos Space Platform. Users in the workspace of an upgraded application are directed to Application Chooser.

RELATED DOCUMENTATION

Managing Junos Space Applications | 1343

Upgrading Junos Space Network Management Platform Overview

IN THIS SECTION

- Before You Begin | 1330
- Pre-Upgrade Checks | 1331
- How an Upgrade Impacts Previously Installed Junos Space Applications | 1331
- Performing the Upgrade | 1332

To upgrade Junos Space Platform, you upload the Junos Space Platform image file to your existing fabric and perform the upgrade using the Junos Space Platform UI. When you perform an upgrade, all nodes in the Junos Space fabric are upgraded to the new software version.

CAUTION: If you are upgrading to Junos Space Platform Release 16.1R1, follow the procedure outlined in Upgrading to Junos Space Network Management Platform Release 16.1R1.

NOTE: For information about the features and updates for a specific Junos Space Platform release, refer to the *Junos Space Network Management Platform Release Notes* for that release.

This topic has the following sections:

Before You Begin

Before you upgrade Junos Space Platform, ensure that you are aware of the following:

- Some Junos Space applications may not support a direct upgrade of Junos Space Platform from Release 16.1R1, Release 16.1R2, or Release 16.1R3 to Release 17.2R1; upgrading to Junos Space Platform Release 17.1R1 may be required before upgrading to Release 17.2R1 for some upgrade scenarios. Therefore, review the release notes for all installed Junos Space applications prior to upgrading Junos Space Platform.
- Upgrading Junos Space Platform clears existing user preferences (set using the **User Settings** global action icon in the Junos Space banner).

- Back up all your Junos Space Platform data before you begin the upgrade process. See "Backing Up the Junos Space Network Management Platform Database" on page 1308 for details to back up data before starting the upgrade process.
- Download the Junos Space Platform Upgrade image from the Junos Space Network Management Platform Download Software page.

CAUTION: Do not modify the filename of the software image that you download from the Juniper Networks support site; if you modify the filename, the upgrade fails.

- You must log in as the default Super Administrator or System Administrator to upgrade Junos Space Platform.
- Before you upgrade Junos Space Platform, ensure that the time on all Junos Space nodes is synchronized. For information about synchronizing time on Junos Space nodes, see "Synchronizing Time Across Junos Space Nodes" on page 1384.

Pre-Upgrade Checks

From Junos Space Platform Release 15.1R1 onward, the system checks for the following before you can upgrade the software:

- Free disk space—If a node or a cluster fails to meet the minimum disk requirement, an error message is displayed. The minimum available disk space required is 10 GB in the / partition. The error message lists the IP address of the node that fails to meet the requirement. If you receive this error message, you cannot continue the upgrade.
- MySQL replication and PostgreSQL replication—If the MySQL replication or PostgreSQL replication processes are turned off on any of the nodes, a warning message is displayed. Junos Space Platform checks the for Mysql, Mysql_Slave_IO, and Mysql_Slave_sql (MySQL) processes and postgres_sender, postgres_receiver, and postgresql (PgSQL) processes to obtain the status of the replication processes. The warning message lists the processes that are down. If you receive only this warning message, you can either continue or stop the upgrade.

If both the preceding checks fail, an error message is displayed that lists all the preceding information. The upgrade process is not initiated.

How an Upgrade Impacts Previously Installed Junos Space Applications

Junos Space Platform provides the running environment for all Junos Space applications. Hence, the operations of the applications are interrupted during the upgrade. Only the applications that are supported on the version of Junos Space Platform to which you are upgrading are enabled. Other applications running

on versions of Junos Space Platform prior to the version to which you are upgrading and that are not supported on that version might be disabled. You must upgrade these disabled applications to the respective compatible version.

NOTE: Do not add disabled Junos Space applications using the Add Application page (**Administration** > **Applications** > **Add Application**).

CAUTION: Refer to the *Upgrade Instructions* section in the *Junos Space Network Management Platform Release Notes* for a specific release to find out the versions of Junos Space Platform that are supported for upgrade.

Performing the Upgrade

Complete the steps outlined in "Upgrading Junos Space Network Management Platform" on page 1378 to upgrade your current Junos Space Platform software to the latest software version.

NOTE: If you are upgrading to Junos Space Platform Release 16.1R1, follow the procedure outlined in Upgrading to Junos Space Network Management Platform Release 16.1R1.

After Junos Space Platform is upgraded, validate that upgrade was successful by logging in to the Junos Space UI.

NOTE: You can view the version of the installed Junos Space Platform software, click the Help icon on the Junos Space banner and in Help sidebar, click **About**.

RELATED DOCUMENTATION

Managing Junos Space Applications Overview | 1328

Managing Junos Space Applications | 1343

Junos Space Store Overview

IN THIS SECTION

- About the Junos Space Store | 1333
- Benefits of Junos Space Store | 1333

About the Junos Space Store

From Junos Space Network Management Platform Release 18.2 onward, you can install and upgrade Junos Space applications from Junos Space Store. Junos Space Store is a repository that lists the latest and supported versions of Junos Space applications.

Junos Space Store enables easy installation of Junos Space applications (including Junos Space application components) from within Junos Space Platform. When you install an application from Junos Space Store, Junos Space Platform downloads the application and installs it instead of requiring you to download it to the local file system from the Juniper Networks software download site: https://www.juniper.net/support/products/space/#sw. If you try to select an incompatible version of a Junos Space application, a warning message appears, indicating that the application version that you are trying to install or upgrade is not compatible with the installed Junos Space Platform version. For more information, see "Configuring and Managing Junos Space Store" on page 1334.

You can also view the versions for each application that are compatible with the installed version of Junos Space Platform and whether or not different applications can coexist within Junos Space Platform.

Alternatively, you can download the applications from the Juniper Networks software download site, and add it to Junos Space Platform by using the existing workflow. For more information, see "Adding a Junos Space Application" on page 1372.

Benefits of Junos Space Store

- You can access information about Junos Space application versions and verify the supported versions from within Junos Space Store, and thus do not need to refer to external resources.
- As you can install and upgrade applications directly from Junos Space Store, you save the time and effort needed to manually download application images from the Juniper Networks software download site and upload them to Junos Space Platform for installation.
- You can configure application components from within Junos Space Store.

SEE ALSO

Configuring and Managing Junos Space Store | 1334
Adding a Junos Space Application | 1372
Upgrading a Junos Space Application | 1376
Uninstalling a Junos Space Application | 1406

Configuring and Managing Junos Space Store

IN THIS SECTION

- Configuring Junos Space Store in Junos Space Network Management Platform | 1334
- Modifying Junos Space Store Settings | 1335
- Installing and Upgrading Junos Space Applications from Junos Space Store | 1336

From Junos Space Network Management Platform Release 18.2 onward, you can install and upgrade Junos Space applications from Junos Space Store. Junos Space Store is a repository that lists the latest and supported versions of Junos Space applications. For more information about Junos Space Store, see "Junos Space Store Overview" on page 1333.

Configuring Junos Space Store in Junos Space Network Management Platform

Before you install Junos Space applications from Junos Space Store, you must configure Junos Space Store in Junos Space Platform.

To configure Junos Space Store in Junos Space Platform:

1. On the Junos Space Platform UI, select **Administration** > **Applications** > **Junos Space Store**.

   The Junos Space Store welcome page appears.

2. Click **Next** to proceed.

   The Junos Space Store page appears with the following message:

   Configure Juniper Networks software download credentials to connect to Junos Space Store.

3. Click **Go To Settings**.

The settings page for Junos Space Store appears with the following message.

Provide Juniper Networks software download credentials to access Junos Space Store repository.

4. Enter your Juniper Networks software download credentials in the appropriate fields.

   NOTE: The proxy server is displayed as enabled or disabled based on the settings you configured on the Administration > Proxy Server page.

5. Click **Test Connection** to test the connection between Junos Space Platform and the Junos Space Store.

   If the connection is successful, the Connection Successful page appears.

   If the test connection fails, an error message is displayed. To proceed, check your proxy server settings and your network connection.

6. Click **Submit** on the settings page to save the Junos Space Store credentials.

   The credentials are saved in Junos Space Store.

7. Click **Go to Junos Space Store**.

   The Junos Space Store page appears, listing all the active Junos Space applications, along with the latest revision and the release date of the latest revision, on the left of the page. When you click an application, the latest and other supported versions of the application are listed on the right of the page.

   NOTE: You need to configure Junos Space Store settings only when you access it for the first time. However, you can modify the settings when required by clicking **Settings** on the Junos Space Store page.

Modifying Junos Space Store Settings

To modify Junos Space Store settings in Junos Space Platform:

1. On the Junos Space Platform UI, select **Administration** > **Applications** > **Junos Space Store**.

   The Junos Space Store page appears.

2. Click **Settings**.

   The settings page for Junos Space Store appears with the following message.

Provide Juniper Networks software download credentials to access Junos Space Store repository.

3. Modify the existing credentials.

   NOTE: The proxy server is displayed as enabled or disabled based on the settings you configured on the Administration > Proxy Server page.

4. (Optional) Click **Test Connection** to test the connection between Junos Space Platform and Junos Space Store.

   If the connection is successful, the Connection Successful page appears.

   If the test connection fails, an error message is displayed. To proceed, check your proxy server settings and your network connection.

5. Click **Submit** on the settings page to save the modified Junos Space Store credentials.

   The credentials are modified and saved in Junos Space Store.

Installing and Upgrading Junos Space Applications from Junos Space Store

To install or upgrade a Junos Space application from Junos Space Store, you must be assigned the appropriate privileges to manage Junos Space Store.

To install and upgrade Junos Space applications from Junos Space Store:

1. On the Junos Space Platform UI, select **Administration** > **Applications** > **Junos Space Store**.

   The Junos Space Store page appears.

2. (Optional) Click **Get Latest** to refresh the list of applications in Junos space Store.

   The list of applications in Junos Space Store gets refreshed, displaying the most recently released versions of Junos Space applications.

3. Select the Junos Space application that you want to install or upgrade by clicking its displayed name.

   The details of the selected application, including the name, description, and release highlights of the application, appear. The version number and release date of the latest versions are also displayed.

   If the application is already installed in Junos Space Platform, the currently installed version is also displayed.

   If the selected version is already installed in Junos Space Platform, a warning message is displayed.

If the selected version is not compatible with the version of Junos Space Platform, a warning message is displayed.

If the selected application cannot coexist with another application that is already installed in Junos Space Platform, an error message is displayed. For example, Network Director and Connectivity Services Director cannot coexist.

4. To view only the versions of the selected application compatible with Junos Space Platform, select the **Show only compatible version** check box above the version table.

   The table gets refreshed and then displays only the compatible versions of the selected application.

5. Select the version of the application that you want to install or upgrade from the listed application versions.

6. Click **Next** to install or upgrade the selected application.

   The End User License Agreement for the selected application appears.

   > **NOTE:** You can configure the components of a Junos Space application from Junos Space Store.
   >
   > Upgrade of components of a Junos Space application is not supported in Junos Space Store. See the respective application documentation for more information.

7. Review the license agreement.
   - Click **Accept and Install** to install the application.
   - Click **Accept and Upgrade** to upgrade the application.

   The detailed job status appears.

8. Click **Go to Junos Space Store** to go back to the Junos Space Store page. The installation or upgrade process continues in the background.

   You can view the progress of the installation or upgrade when you select the application listed in Junos Space Store.

NOTE: You can modify Junos Space Store settings by clicking **Settings** in Junos Space Store.

You can initiate the installation or upgrade of a Junos Space application while another installation or upgrade is still in progress. The newly initiated process will automatically begin after the currently running process is completed.

RELATED DOCUMENTATION

- Junos Space Store Overview | 1333
- Adding a Junos Space Application | 1372
- Upgrading a Junos Space Application | 1376
- Uninstalling a Junos Space Application | 1406

Running Applications in Separate Server Instances

IN THIS SECTION

- Adding a Server Group | 1339
- Adding a Server to a Server Group | 1340
- Starting Servers in a Server Group | 1341
- Stopping Servers in a Server Group | 1341
- Removing a Server Group | 1342
- Moving an Application to a Different Server Group | 1342

Junos Space enables you to deploy an application to a separate instance within an application server so that you can allocate resources to each application. You can individually shut down an instance without affecting other instances that are running other applications.

Junos Space Release 13.3R1 and later versions run on JBoss EAP 6, which supports the concept of a managed domain. A domain comprises one or more server groups and each server group comprises one or more server instances. A domain is controlled by a domain controller, which ensures that each server is configured according to the management policy of the domain. With this feature, you can deploy each

application to a separate server instance, if needed. You can also shut down individual instances without affecting other instances that are running other applications.

Before you install Junos Space Network Management Platform, it is necessary that you set up the infrastructure of server groups and add servers to the server groups so that you can install an application such as Security Director on a specific server instance. After the setup is ready, add the application from the Junos Space UI (see "Adding a Junos Space Application" on page 1372).

> **NOTE:** Service Now and Service Insight should be run in the same server group of a JBoss EAP domain as the Junos Space Network Management Platform. Operating Service Now, Service Insight, and Junos Space Network Management Platform in different server groups is not supported.

Instructions to set up, start, stop, or remove a server instance are in the following topics:

Adding a Server Group

A server group comprises one or more server instances that are managed and configured as one. All servers (server instances) of the same server group perform the same tasks because they share the same profile configuration and deployed content.

To add a server group:

1. Launch the management CLI in Linux by typing the following text at the command prompt:
   EAP_HOME/bin/jboss-cli.sh

2. Type the following text:
   $sh jboss-cli.sh --connect --controller=<*DOMAIN_CONTROLLER_HOST*>
   "/server-group=<*SERVER_GROUP_NAME*>:add(profile=full-ha,socket-binding-group=full-ha-sockets)"

   In this text:

   - *DOMAIN_CONTROLLER_HOST* is the hostname of the server that runs Junos Space Network Management Platform.
   - *SERVER_GROUP_NAME* is the name of the server group that you want to add.

   > **NOTE:** Refer to the JBoss version 6 documentation set for more information about configuring the **profile** and **socket-binding-group** parameters.
   >
   > The configuration in this topic provides you with full clustering capabilities because you have used the **profile=full-ha** parameter at the command prompt.

For the newly added server group to appear in the Junos Space GUI:

1. From the shell console, enter **/var/cache/jboss/jmp/payloads/**.

2. Navigate to the directory in which you have installed the application. For example, **/var/cache/jboss/jmp/payloads/ICEAAA.xxxxx/**.

3. Open the **swIndex.txt** file and add the following text: **IsOnlyDeployedWithPlatform=false**.

Adding a Server to a Server Group

You should add a new server to a server group so that you can run an application separately on this server. However, when you install Junos Space Network Management Platform, by default a **platform** server group is created and all the applications are added to this server group automatically.

To add a server to a server group:

1. Launch the management CLI in Linux by typing the following text at the command prompt: **EAP_HOME/bin/jboss-cli.sh**

2. Type the following text:
   $sh jboss-cli.sh --connect --controller=<*DOMAIN_CONTROLLER_HOST*>
   "/host=<*HOSTNAME*>//server-config=<*SERVER_NAME*>:add(auto-start=true,
   group=<*SERVER_GROUP_NAME*>, socket-binding-port-offset=100)"

   In this text:

   - *DOMAIN_CONTROLLER_HOST* is the hostname of the server that run the Junos Space Network Management Platform.
   - *HOSTNAME* is defined in host.xml in the **/usr/local/jboss/domain/configuration** directory.
   - *SERVER_NAME* is the name of the server that you want to add.
   - *SERVER_GROUP_NAME* is the name of the server group to which you want to add the new server.

   NOTE: Refer to the JBoss version 6 documentation set for more information about configuring the **auto-start** and **socket-binding-port-offset** parameters.

NOTE: After you have successfully added a server to a server group (for example, consider you have added a server group called as firstServerGrp), log in to the domain controller and perform the following action:
/server-group= *firstServerGrp*/jvm= *firstServerGrp*/:add(max-heap-size=1024m,max-permgen-size=256m,heap-size=64m)

Starting Servers in a Server Group

You need to start a server in a server group before you deploy an application to this server instance.

To start a server in a server group:

1. Launch the management CLI in Linux by typing the following text in a command line:
   EAP_HOME/bin/jboss-cli.sh

2. Type the following text:
   $sh jboss-cli.sh --connect --controller=<*DOMAIN_CONTROLLER_HOST*>
   "/server-group=application/:start-servers".
   In this text, *DOMAIN_CONTROLLER_HOST* is the hostname of the server that runs Junos Space Network Management Platform.

   This command starts all servers in a server group.

   To start a specific server, use the following command:
   $sh jboss-cli.sh --connect --controller=<*DOMAIN_CONTROLLER_HOST*>
   "/host=<*HOSTNAME*>server-config=<*SERVER_NAME*>/:start(server=<*SERVER_NAME*>,blocking=false)"

Stopping Servers in a Server Group

You may want to stop the servers within a server group when you no longer need them—for example, in situations where no applications are running on these servers.

To stop a server in a server group:

1. Launch the management CLI in Linux by typing the following text in a command line:
   EAP_HOME/bin/jboss-cli.sh

2. Type the following text:
   $sh jboss-cli.sh --connect --controller=<*DOMAIN_CONTROLLER_HOST*>
   "/server-group=application/:stop-servers"
   In this text, *DOMAIN_CONTROLLER_HOST* is the hostname of the server that runs Junos Space Network Management Platform.

This command stops all the servers in a server group.

To stop a specific server, use the following command:
$sh jboss-cli.sh --connect --controller=<*DOMAIN_CONTROLLER_HOST*>
"/host=<*HOSTNAME*>server-config=<*SERVER_NAME*>/:stop(server=<*SERVER_NAME*>,blocking=false)"

Removing a Server Group

You may want to remove a server group when you no longer need it—for example, in situations where no applications are running on these server groups.

To remove a server group:

1. Launch the management CLI in Linux by typing the following text in a command line:
   EAP_HOME/bin/jboss-cli.sh

2. Type the following text:
   $sh jboss-cli.sh --connect --controller=<*DOMAIN_CONTROLLER_HOST*>
   "/server-group=<*SERVER_GROUP_NAME*>:remove"

   In this text:

   - *DOMAIN_CONTROLLER_HOST* is the hostname of the server that runs Junos Space Network Management Platform.
   - *SERVER_GROUP_NAME* is the name of the server group that you want to remove.

Moving an Application to a Different Server Group

You can move an application from the current server group to a different server group, if needed, by using the moveApplication.pl script under the **/var/www/cgi-bin** directory.

> **NOTE:** Before moving an application to another server group (for example, to secondServerGrp), log in to the domain controller and perform the following action:
> **/server-group= *secondServerGrp*/jvm= *secondServerGrp*/:add(max-heap-size=1024m,max-permgen-size=256m,heap-size=64m)**

To move an application from the current server group to another server group:

1. From the shell console, enter **/var/www/cgi-bin**.

2. Type the following text:

$perl moveApplication.pl -s <*SOURCE_SERVER_GROUP*> -d <*DESTINATION_SERVER_GROUP*> -a <*APPLICATION_NAME*>

- SOURCE_SERVER_GROUP is the name of the server group from which you want to remove the application.
- DESTINATION_SERVER_GROUP is the server group that want to move the application to.
- APPLICATION_NAME is the name of the application that want to move from the current server group to another server group.

For example, to move the ICEAAA application from firstServerGrp to secondServerGrp, type the following text:
moveApplication.pl -s firstServerGrp -d secondServerGrp -a ICEAAA

RELATED DOCUMENTATION

Uninstalling a Junos Space Application | 1406

Managing Junos Space Applications

IN THIS SECTION

- Viewing Detailed Information About Junos Space Platform and Applications | 1344
- Performing Actions on Junos Space Platform and Applications | 1344

You can manage Junos Space Network Management Platform and Junos Space applications from the Applications page (**Administration** > **Applications**). All Junos Space applications that you have uploaded and installed appear on the Applications page. You must have Super Administrator or System Administrator privileges to manage Junos Space Platform and Junos Space applications.

From the Applications page, you can perform actions on Junos Space hot-pluggable applications, such as installation, upgrading, and uninstallation, while Junos Space Platform is still running.

This topic contains the following sections:

Viewing Detailed Information About Junos Space Platform and Applications

Table 164 describes the information displayed in table columns for Junos Space Platform and each Junos Space application on the Applications page.

Table 164: Application Information

Application Information	Description
Title	Name of the Junos Space application; for Junos Space Platform, **Network Management Platform** is displayed.
Version	Version number of Junos Space Platform or Junos Space application
Release Type	Release type of Junos Space Platform or the Junos Space application; for example, R1.
Build	Build number of Junos Space Platform or the Junos Space application
Server Group	Server group to which the application belongs. For more information on server group, see "Running Applications in Separate Server Instances" on page 1338. By default, all applications belong to the **platform** server group unless you added an application to another server group. For more information about adding an application to a server group, see "Adding a Junos Space Application" on page 1372.

Performing Actions on Junos Space Platform and Applications

You can perform the following actions on the Junos Space applications from the Actions menu. You must first select an application before you can perform an action on it from the Actions menu. You can also right-click an application to perform these actions.

- **Modify Application Settings**—See "Modifying Settings of Junos Space Applications" on page 1345 and "Modifying Junos Space Network Management Platform Settings" on page 1346.
- **Refresh Search Index**—Click to refresh the search index to keep it current with the changes made to the database. By default, the search index is refreshed every five seconds. You can modify this duration from **Administration > Applications > Network Management Platform > Modify Application Settings > Search > Index auto update interval in seconds**. You are prompted to confirm that you want to refresh the search index. Click **OK** to confirm.
- **Manage Services**—See "Starting, Stopping, and Restarting Services" on page 933.
- **Upgrade Platform**—See "Upgrading Junos Space Network Management Platform" on page 1378.

> **NOTE:** This action is available for Junos Space Platform only.

- **Upgrade Application**—See "Upgrading a Junos Space Application" on page 1376.
- **Uninstall Application**—See "Uninstalling a Junos Space Application" on page 1406.
- **Delete Private Tags**—Delete private tags; that is, delete tags that you created.
- **Tag It**—See "Tagging an Object" on page 1526.
- **Untag It**—"Untagging Objects" on page 1527.
- **View Tags**—See "Viewing Tags for a Managed Object" on page 1532.

RELATED DOCUMENTATION

Managing Junos Space Applications Overview | 1328

Junos Space Store Overview | 1333

Configuring and Managing Junos Space Store | 1334

Running Applications in Separate Server Instances | 1338

Upgrading Junos Space Network Management Platform Overview | 1330

Modifying Settings of Junos Space Applications

As the Super Administrator or System Administrator, you can modify the settings of installed Junos Space applications.

> **NOTE:** For information on how to modify the settings of Junos Space Network Management Platform, refer to "Modifying Junos Space Network Management Platform Settings" on page 1346.

To modify the settings of a Junos Space application:

1. On the Junos Space Platform UI, select **Administration** > **Applications**.

   The **Applications** page is displayed with the list of installed Junos Space applications.

2. Select the Junos Space application whose settings you want to modify.

   > **NOTE:** You cannot modify the application settings for Junos Space Service Now and Junos Space Service Insight

3. Select **Modify Application Settings** from the Actions menu or the shortcut menu.

   The settings page for the Junos Space application that you selected is displayed. For more information on modifying settings for a Junos Space application, refer to the documentation for that Junos Space application.

   NOTE: You cannot modify the application settings if another user is currently modifying the application settings. You receive a pop-up message indicating the user who is currently modifying the application settings.

RELATED DOCUMENTATION

- Managing Junos Space Applications Overview | 1328
- Managing Junos Space Applications | 1343
- Uninstalling a Junos Space Application | 1406
- Upgrading a Junos Space Application | 1376

Modifying Junos Space Network Management Platform Settings

As the Super Administrator or System Administrator, you can modify the settings of Junos Space Network Management Platform.

To modify the settings of Junos Space Platform:

1. On the Junos Space Platform UI, select **Administration** > **Applications**.

   The **Applications** page is displayed.

2. Select **Network Management Platform**.

3. Select **Modify Application Settings** from the Actions menu or right-click Network Management Platform and select **Modify Application Settings**.

   The Modify Application Settings (Modify Network Management Platform Settings) page is displayed and the Device section is selected by default.

NOTE:

- You cannot modify the application settings if another user is currently modifying the application settings. You receive a pop-up message indicating the user who is currently modifying the application settings.
- For the Junos Space Platform settings that have numerical values, the label **[Default]** is displayed to the right of the text box if the value is the system default.
- In each section of the Modify Application Settings (Modify Network Management Platform Settings) page, the settings that you modified are automatically saved from Junos Space Network Management Platform Release 17.1R1 onward.

  The settings are saved only temporarily so that you can change the settings in other sections. To save the settings across sections, you must explicitly click the **Modify** button; for more information, see 15.

4. (Optional) Modify the settings related to the devices, as shown in Table 165.

Table 165: Device Settings

Field	Description
Add SNMP configuration to device for fault monitoring	This check box is selected by default, which ensures that the SNMP target for the devices that are discovered from Junos Space Platform is set to the Junos Space VIP node. This configuration enables these devices to send their SNMP traps to the Junos Space VIP node. If you clear the check box, then SNMP trap targets are not set for the devices that are newly added in Junos Space Platform. The devices whose SNMP trap targets are not set do not send their SNMP traps to the Junos Space VIP node.
Allow Device Communication	This check box enables discovered devices to communicate with the Junos Space server. If the check box is cleared, the discovered devices cannot communicate with the Junos Space server.
Allow users to auto log in to devices using SSH	This check box allows users to automatically log in when starting an SSH connection on a device. The default (check box is cleared) indicates that you have to add your credentials to log in to a device using SSH.
Auto resync device	This check box ensures that when the network is the system of record, configuration changes on a connected Juniper Networks device are synchronized with or imported to the application database. By default, this check box is selected.

Table 165: Device Settings *(continued)*

Field	Description
Configure commit synchronize during device discovery	This check box ensures that for either system of record, configuration changes in Junos Space Platform for a device are pushed, committed, and synchronized during device discovery. By default, this check box is selected.
Disable network monitoring for all devices	This check box determines whether Network Monitoring is used to monitor only Junos Space fabric nodes (check box is cleared) or both Junos Space fabric nodes and devices (check box is selected): **NOTE:** This check box is cleared by default. 1. If the **Disable network monitoring for all devices** check box is selected, then during device discovery Junos Space Platform does *not* push SNMP trap targets to devices or add devices into Network Monitoring. In addition, if a Resync Nodes job is triggered, Junos Space Platform removes devices that are already present in Network Monitoring and removes the trap target settings that were previously set on the devices. In addition, Junos Space Platform does not synchronize additional devices with the Network Monitoring workspace. 2. If the **Disable network monitoring for all devices** check box is cleared, Junos Space Platform does the following: • Pushes the SNMP trap targets to the devices during the discovery of new devices if the **Add SNMP configuration to device for fault monitoring** check box is selected If the **Add SNMP configuration to device for fault monitoring** check box is cleared, then the SNMP trap targets are not pushed to the devices. • Adds the device into Network Monitoring during the discovery of new devices **NOTE:** For devices that are added to Junos Space Platform before the **Disable network monitoring for all devices** check box is cleared, you must initiate a manual device resynchronization to add the devices into Network Monitoring. 3. If the **Disable network monitoring for all devices** check box was previously cleared and is changed to selected, then you must trigger a manual device resynchronization so that Junos Space Platform removes the devices from Network Monitoring. The rest of the behavior is the same as explained in the first step.
System of Record Settings	This setting enables you to specify whether the network is the system of record (NSOR, which is the default) or whether Junos Space Platform is the system of record (SSOR). **NOTE:** Resynchronization choices on this page apply only to NSOR.
Enable approval workflow for configuration deployment	This option is for a candidate configuration (previously known as consolidated configuration) and lets a user deploy any configuration changes made from Junos Space Platform on to a device only on approval. By default, this check box is selected. By clearing this check box, you can deploy the configuration directly without approval.

Table 165: Device Settings *(continued)*

Field	Description
Enable commit confirmed for configuration deployment	Specify that the device waits for a specified time for the configuration to be explicitly committed when a commit configuration request is sent from Junos Space Platform. The default wait time is 10 minutes. This check box is cleared by default.
Junos Space initiates connection to device	This check box is selected by default, so Junos Space Platform initiates a connection with managed devices. To have managed devices initiate a connection with Junos Space Platform, clear this check box.
Looking Glass Device response timeout in secs	Specify a timeout interval for devices on which the looking glass feature is applied. Junos Space Platform waits until the specified timeout interval for a response has lapsed and if there is no response, the request is timed out. The minimum timeout interval is 30 seconds, the maximum is 600 seconds, and the default is 120 seconds.
Max auto resync waiting time secs	This field specifies the initial time within which device configuration changes are synchronized with the database. If multiple commit logs are received from devices, Junos Space waits for this time interval to lapse before the resynchronization of the device configuration is initiated. The default waiting time is 20 seconds. This setting is applicable only when the network is the system of record.
Number of devices to connect per minute for Space Initiated Connection	This parameter enables you to control the number of devices connecting with Junos Space Platform. The default number of devices allowed to connect per minute in connections initiated by Junos Space Platform is 500 devices and the maximum number of devices is 1000. If Junos Space Platform connects to too many devices simultaneously, the performance of the network is weakened.
Polling time period secs	This setting is for specifying the interval at which to poll the configuration of devices that do not support system logging (non-Junos OS devices). Junos Space Platform polls and compares the configuration it has with that of the device at the interval set here. If there is a difference, it is reported. If the network is the system of record, Junos Space Platform synchronizes its configuration with that on the device. The default is 900 seconds.
SSH port for device connection	This field specifies the SSH port on the device. Junos Space Platform uses this port to discover devices. The default value, 22, is the standard SSH server port.

Table 165: Device Settings *(continued)*

Field	Description
Enable abort rpc call for timed out sessions	Enabling this option calls **<abort/>** rpc for timed out NETCONF sessions. If this option is not enabled, **<close-session/>** rpc is used to close all NETCONF sessions. The difference in behavior applies only to timed out or terminated sessions.
Manually Resolve Fingerprint Conflict	When a fingerprint conflict occurs during device reconnection or when a user connects to a device by using the secure console or SSH, Junos Space Platform allows the user to resolve a fingerprint conflict manually or resolves the conflict automatically. This check box is selected by default, which means that the user must resolve the fingerprint conflict manually. If the check box is cleared, Junos Space Platform resolves the fingerprint conflict automatically by accepting the fingerprint that is presented during authentication. **NOTE:** If Junos Space Platform maintains an active connection with a device, the change in the device fingerprint is not recognized by Junos Space Platform. Fingerprint changes on devices are recognized when the devices reconnect with Junos Space.
Support WW Junos Devices	Select this check box to enable support for devices running worldwide Junos OS (ww Junos OS devices) and clear the check box to disable support for ww Junos OS devices. This check box is cleared by default.

5. (Optional) Click the **User** hyperlink (on the left of the page) to modify the settings related to users, as shown in Table 166.

Table 166: User Settings

Field	Description
Automatic logout after inactivity (minutes)	Specify the time, in minutes, after which a user who is idle (that is, has not performed any action such as pressing a key or clicking a mouse) is automatically logged out of Junos Space Platform. This setting conserves server resources and protects the system from unauthorized access. The default value for this setting is five minutes. From Release 17.1R1 onward, you can set a value of up to 480 minutes. If you set the configuration to **Never**, the idle time out is disabled and the user is never logged out of Junos Space Platform due to inactivity. **NOTE:** From Release 17.1R1 onward, you can override this setting by specifying a user-specific value when you create or modify a user account.

Table 166: User Settings *(continued)*

Field	Description
Disable inactive user after time period (Days)	Specify the number of days after which a user who is inactive (a user who has not performed any action such as pressing a key or clicking the mouse) is automatically disabled in Junos Space Platform. The **Disable inactive user after time period (Days)** setting is available from Release 16.1R1 onward. This setting protects the system from unauthorized access. A user who is disabled cannot log in to Junos Space Platform. To enable the user to log in again, use the Enable Users action on the User Accounts page of the Role-Based Access Control workspace. By default, the time period is set to Never, which means the user is never disabled because of inactivity. You can choose a period of up to 120 days to permit a user to be inactive, after which the user is disabled. If an SMTP server and the user's e-mail address are configured, an e-mail notification about account disabling is sent to the user 24–48 hours before the user account is disabled.
Maximum concurrent UI sessions per user	Specify the number of concurrent user sessions allowed per user for GUI login at the global level (that is, for all users). The default value is 5. You can enter a value from 0 (zero) through 999. Entering 0 (zero) means that there are no restrictions on the number of concurrent UI sessions allowed per user. However, the system performance may be affected if you allow unlimited concurrent UI sessions. **NOTE:** • If you are a super user, this concurrent user session limit does not apply and you are allowed to log in even when you have exceeded this limit. • The changes that you make to the concurrent UI sessions limit (either at the global level or at the user level) do not affect existing sessions; this limit is validated against the next user login only.
UI auto refresh interval in seconds	Specify the time, in seconds, after which the Junos Space GUI is refreshed automatically. The default value is 3 seconds.
Use User Password Auth Mode choices	• **Use User Password Auth Mode**—Select this option, which is the default, if you want the Junos Space server to authenticate the user on the basis of username and password entered by the user. • **Use X509 Certificate Complete Certificate**—Select this option if you want the Junos Space server to authenticate the user on the basis of the certificate of the user. • **Use X509 Certificate Parameters**—Select this option if you want the Junos Space server to authenticate the user on the basis of the X.509 certificate parameters.

For more information about changing authentication modes, refer to "Changing User Authentication Modes" on page 1434.

> **NOTE:** If you change the authentication mode from password-based to certificate-based by using the **Use X509 Certificate Complete Certificate** option without uploading appropriate certificates or from certificate-based to certificate parameter–based by using the **Use X509 Certificate Parameters** option without adding and activating the parameters, an error message is displayed in a pop-up window. Click **OK** to close the pop-up window.

6. (Optional) Click the **Password** hyperlink (on the left of the page) to modify the settings related to password rules, as shown in Table 167.

> **NOTE:** You click the **User Settings** icon on the Junos Space banner (see "Changing Your Password on Junos Space" on page 177) to change your password, but the constraints that govern the password are set on the Modify Application Settings (Modify Network Management Platform Settings) page.

Table 167: Password Settings

Field	Description
Advanced Settings	To view or configure advanced password settings, click the **view/configure** hyperlink. You are taken to the **Password > Advanced Settings** section. Refer to step a for details.
Minimum no. of characters	Specify the minimum number of characters that a password must contain. The minimum value for this field is 6 (the default) and the maximum value is 999.
No. of previous passwords cannot be reused	Specify the number of previous passwords that cannot be reused when users change their passwords. For example, if you enter **10**, users cannot reuse any of their previous 10 Junos Space Platform passwords. The range is 0 (zero) through 999 and the default is 6; 0 (zero) indicates that there is no restriction on password reuse.

Table 167: Password Settings *(continued)*

Field	Description
No. of unsuccessful attempts before lockout	Specify the number of successive attempts after which Junos Space Platform locks out users who enter incorrect passwords. Junos Space Platform identifies users by their IP addresses, so that even if users have exceeded the limit for incorrect passwords on one system they can try to log in again from a different system. The range is 0 (zero) through 999 and the default is 4; 0 (zero) means that users are not locked out due to login failures. **NOTE:** This verification applies only to users who are in the Junos Space Platform database. It does not work with RADIUS and TACACS+ server authentication.
Time interval for lockout in hours	Specify the interval (in hours) for which a user who has entered incorrect passwords more than the number of times specified in **No. of unsuccessful attempts before lockout** is locked out. The range is 0 (zero) through 999 and the default is 12 (hours); 0 (zero) means that users are never locked out. **NOTE:** You can unlock a locked-out user at any time (see "Disabling and Enabling Users" on page 1051).
Time interval for password expiry in months	Specify the duration (in months) after which passwords of all the locally authenticated Junos Space Platform users expire. The range is 0 (zero) through 999 and the default is 3; 0 (zero) means that the passwords never expire. **NOTE:** • This configuration does not have any impact on the RADIUS or TACACS+ server–authenticated users. • If you upgrade to Junos Space Release 13.1 or later, the password expiry time of the existing local users remain as is until the users modify their passwords or you change the value in this field.

Table 167: Password Settings *(continued)*

Field	Description
Time interval for password expiry notification in months	Specify the number of months in advance that users are warned that their passwords will expire. For example, if you enter **2**, users receive a notification two months before their current passwords expire. The range is 0 (zero) through 999 and the default is 1 (month). Make sure that the value you enter here is less than or equal to the value in the **Time interval for password expiry in months** field.

a. (Optional) Modify the fields related to advanced password settings as explained in Table 168.

Table 168: Advanced Password Settings

Field	Description
At least one lowercase character	Specify whether at least one lowercase letter is required in the password. This check box is selected by default.
At least one number not in the last position	Specify that the password must contain at least one number and that a number cannot be the last character of the password. This check box is selected by default. When this check box is selected, a password that contains a number as the last character is not allowed.
At least one special character not in the last position	Specify that the password must contain at least one special character (non-alphanumeric character) and that a special character cannot be the last character of the password. This check box is selected by default. When this check box is selected, a password that contains a special character as the last character is not allowed.
At least one uppercase character	Specify whether at least one uppercase letter is required in the password. This check box is disabled by default.
No more than three repetitive characters	Specify that a password should not contain the same character repeated more than three times in succession; for example, Exam333pl3e and E3x3a3m3ple are valid passwords, whereas Exam3333ple is not. This check box is selected by default.
Not repeat of the user ID	Specify that the username should not be part of the password. This check box is selected by default.
Not reverse of the user ID	Specify that the username in reverse should not be a part of the password. This check box is selected by default.

7. (Optional) Click the **Domain** hyperlink (on the left of the page) to modify the settings related to domains, as shown in Table 169.

Table 169: Domain Settings

Field	Description
Enable users to manage objects from all allowed domains in aggregated view	Specify whether a user can view and manage all objects from all domains to which the user is assigned (check box is selected) or not (check box is cleared, which is the default). For example, when this check box is selected, a user can stage a script belonging to one domain to a device in another domain. A user can override this configuration by setting the preference from the **User Settings** configuration section.
Enable option to manage read/execute access to parent domain objects at time of domain creation	Specify whether users with access to a child domain object can access objects belonging to the parent domain (check box is selected) or not (check box is cleared, which is the default). When this check box is selected, a user with access to child domain objects can perform read and execute actions on parent domain objects. The following objects are accessible: • Device templates and template definitions • CLI Configlets, Configuration Views, and XPath and regular expressions • Images, scripts, operations, and script bundles • Reports and report definitions

8. (Optional) Click the **Audit Log** hyperlink (on the left of the page) to modify the settings related to audit logs, as shown in Table 170.

Table 170: Audit Log Settings

Field	Description
Audit log forwarding interval in minutes	Enter the time interval based on which audit logs will be forwarded according to the audit log forwarding criteria that are configured and enabled. The default time interval for audit log forwarding is 60 minutes.
Log successful audit log forwarding	Select this check box for successful audit log forwarding to be logged. **NOTE:** For more information about forwarding audit logs, see "Audit Log Forwarding in Junos Space Overview" on page 1492.

Table 170: Audit Log Settings *(continued)*

Field	Description
Record HTTP GET method	Select this check box if you want all API GET calls to be logged in the audit log. By default, this check box is cleared. **NOTE:** If this check box is selected, only API GET calls invoked from external scripts are logged; API GET calls originating from the Junos Space Platform user interface or Junos Space applications are never logged.

9. (Optional) Click the **Search** hyperlink (on the left of the page) to modify the settings related to search, as shown in Table 171.

Table 171: Search Settings

Field	Description
Index auto update interval in seconds	Specify the interval (in seconds) for automatic updates to the index. The default is five seconds, which means that for every five seconds the system automatically checks whether there are any new changes in the database that need to be indexed.
Index page interval in hours	Specify the index page interval in hours. The default is two hours. This field determines the interval at which Junos Space Platform reindexes objects in the database. For example, if you specified the index page interval as three hours on 23-Dec-2014 at 4:00 PM (current date and time) and that the last indexing was completed at 1:00 PM on 22-Dec-2014, because the last indexing was performed more than three hours ago, Junos Space Platform indexes objects from 1:00 PM on 22-Dec-2014 to 4:00 PM on 22-Dec-2014 and marks the last index date and time as 22-Dec-2014 4:00 PM. This process is repeated for the specified index page interval—3 hours in this example—until all the objects are indexed. If there is no last index time present in the database, Junos Space Platform uses the date and time of the database creation as the last index time.
Pause indexing during device import	Specify whether indexing should be paused during device import (check box is selected, which is the default) or not (check box is cleared). If you have to discover a large number of devices (for example, in the range of thousands), this setting speeds up the device discovery by approximately 10%.

10. (Optional) Click the **CLIConfiglets** hyperlink (on the left of the page) to modify the settings related to CLI Configlets, as shown in Table 172.

Table 172: CLI Configlet Settings

Field	Description
Advanced XPath Processing	If this check box is selected, whenever you trigger an action on a device that requires BaseX support, the BaseX database is populated for that device across the Junos Space nodes. Any resynchronization or discovery triggered after the configuration is enabled is handled. If this check box is cleared (default), then the BaseX database is not used.
Enable Approval Workflow for Configlets	If this check box is selected, the configuration changes through CLI Configlets for devices are displayed in the Change Summary tab on the Review/Deploy Configuration page in the Devices workspace. You can exclude, include, approve, reject, or delete the changes through CLI Configlets (displayed in curly-braces format) before deploying the configuration changes on the device. If you select this check box, the Apply CLI Configlets workflows in the Devices and CLI Configlets workspace display a Submit button. If this check box is cleared (default), the Submit button is not displayed in the Apply Configlet workflows (in the Devices and CLI Configlets workspaces) and you cannot submit the configuration changes through CLI Configlets. You must apply the CLI Configlets in the Apply Configlet workflows to deploy the configuration changes through CLI Configlets.

11. (Optional) Click the **RESTAPI** hyperlink (on the left of the page) to modify the settings related to REST APIs, as shown in Table 173.

Table 173: REST API Settings

Field	Description
Include detailed results in job completion response	This setting affects how detailed job results data is returned by a hornet-q poll API when a Junos Space job or a "'Long Running Request" is completed. The job results data is always returned in the last hornet-q progress-update response message that has the **<state>** element set to "DONE" and the **<percentage>** set to "100.0"'. If this check box is selected, the last progress-update response returns detailed results in the **<data>** element. If this check box is cleared (default), the last progress-update response returns the detailed results in an href attribute of the **<detail-link>** element along with the type attribute containing the media-type name of the custom job detail. **NOTE:** This setting applies only to those jobs that support "detail-link" reporting (currently, the **/api/space/script-management** and **/api/space/configlet-management** jobs). For other jobs that do not support "detail-link" reporting, the last progress-update response returns detailed results in the **<data>** element or returns the **<data>** element as "No Result Data Available". In both cases, the **<summary>** element contains the summary of job results.

12. (Optional) Click the **Security** hyperlink (on the left of the page) to modify the settings related to HTTPS access to Junos Space Platform through Web browsers or other HTTP clients, as shown in Table 174.

Table 174: Security Settings

Field	Description
Disable weak algorithms for WEB or API access	

Table 174: Security Settings *(continued)*

Field	Description
	This setting affects the type of key exchange, encryption, authentication, and MAC digest algorithms used for HTTPS access to Junos Space Platform through Web browsers and API clients. By default, this check box is not selected. If this check box is selected, only Transport Layer Security (TLS) version 1.2 protocol–compliant Web or API clients can access Junos Space. The TLS 1.2 algorithm is available from Release 16.1R1 onward. Table 175 lists TLS version 1.2 algorithms that are supported for HTTPS access when weak algorithms are disabled. One of the following cipher suites is configured on the Apache Web server depending on whether the corresponding check box is selected or cleared: • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA384 • DHE-DSS-AES256-GCM-SHA384 • DHE-RSA-AES256-GCM-SHA384 • DHE-RSA-AES256-SHA256 • DHE-DSS-AES256-SHA256 • ECDH-RSA-AES256-GCM-SHA384 • ECDH-ECDSA-AES256-GCM-SHA384 • ECDH-RSA-AES256-SHA384 • ECDH-ECDSA-AES256-SHA384 • AES256-GCM-SHA384 • AES256-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA256 • DHE-DSS-AES128-GCM-SHA256 • DHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES128-SHA256 • DHE-DSS-AES128-SHA256 • ECDH-RSA-AES128-GCM-SHA256 • ECDH-ECDSA-AES128-GCM-SHA256 • ECDH-RSA-AES128-SHA256 • ECDH-ECDSA-AES128-SHA256

Table 174: Security Settings *(continued)*

Field	Description
	• AES128-GCM-SHA256 • AES128-SHA256 If this check box is cleared, only the TLS version 1.1 protocol–compliant Web and API clients can access Junos Space. **NOTE:** You can enable or disable weak algorithms only if all load balancers are in the UP state. When you enable or disable weak algorithms, a warning message is sent to all user sessions, the user sessions are stopped, and the users are logged out.

Table 175: Supported TLS Version 1.2 Algorithms for HTTPS Access When Weak Algorithms Are Disabled

Encrypted Connection	Details	MAC
ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(256)	Mac=AEAD
ECDHE-RSA-AES256-SHA384	TLSv1.2 Kx=ECDH Au=RSA Enc=AES(256)	Mac=SHA384
DHE-RSA-AES256-GCM-SHA384	TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256)	Mac=AEAD
DHE-RSA-AES256-SHA256	TLSv1.2 Kx=DH Au=RSA Enc=AES(256)	Mac=SHA256
AES256-GCM-SHA384	TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(256)	Mac=AEAD
AES256-SHA256	TLSv1.2 Kx=RSA Au=RSA Enc=AES(256)	Mac=SHA256
ECDHE-RSA-AES128-GCM-SHA256	TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(128)	Mac=AEAD
ECDHE-RSA-AES128-SHA256	TLSv1.2 Kx=ECDH Au=RSA Enc=AES(128)	Mac=SHA256

Table 175: Supported TLS Version 1.2 Algorithms for HTTPS Access When Weak Algorithms Are Disabled *(continued)*

Encrypted Connection	Details	MAC
DHE-RSA-AES128-GCM-SHA256	TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128)	Mac=AEAD
AES128-GCM-SHA256	TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(128)	Mac=AEAD
AES128-SHA256	TLSv1.2 Kx=RSA Au=RSA Enc=AES(128)	Mac=SHA256

13. (Optional) Click the **HealthMonitoring** hyperlink (on the left of the page) to modify the health monitoring settings related to the System Health Report displayed on the Administration statistics page, as shown in Table 176.

Table 176: Health Monitoring Settings

Field	Description
Enable File System Intrusion Detection Monitoring	Select this check box to enable file integrity check. For more information, see "Managing File Integrity Check" on page 1367.
Interval for monitoring the File Changes in hours	Specify the time interval at which Junos Space Platform should run file integrity check. You can enter a value in hours. By default, this is set to 24 hours. For more information, see "Managing File Integrity Check" on page 1367
Interval for monitoring CPU counters update in minutes	Specify the difference in minutes between the time when the overall load on a Junos Space node and CPU resources shared by processes on the node was last calculated and the system time. Range: One through 120 minutes Default: Two minutes
Interval for monitoring device management session in minutes	Specify an interval in minutes to execute the **netstat -anlp | awk '{print $5}' | grep ":22" | wc –l** command to calculate the device management SSH sessions established between a Junos Space node and the managed devices connected to that node. Range: 10 through 120 minutes Default: 30 minutes

Table 176: Health Monitoring Settings *(continued)*

Field	Description
Device Management Sessions Monitoring Threshold	Specify the tolerance level up to which the difference in the number of device management SSH sessions calculated by using the **netstat -anlp | awk '{print $5}' | grep ":22" | wc –l** command (Number of Devices column) and the number of device management SSH sessions as listed in the Junos Space database (Console Count column) is accepted. When this difference exceeds the specified tolerance level, the Management sessions are mismatched with UI data parameter in the System Health Report displays a red “No”. Range: 0 (zero) through 1000 Default: 10
Disk Utilization Threshold Value in percentage	Specify a percentage of hard disk drive free space above which the usage is considered to be higher than normal usage. Range: 30% through 100% Default: 50%
High CPU Threshold Value in percentage	Specify a percentage of CPU resource usage above which the usage is considered to be higher than normal usage. Range: 30% through 100% Default: 50%
Extended Period for High CPU in minutes	Specify an interval in minutes above which a higher-than-average usage of CPU resources must be reported. Range: 10 through 120 minutes Default: 30 minutes
Interval for monitoring HPROF file in hour	Specify an interval in hours to detect and log the Heap and CPU Profiling Agent (HPROF) files on all Junos Space nodes in the Junos Space fabric. Range: One through 240 hours Default: One hour

Table 176: Health Monitoring Settings *(continued)*

Field	Description
Interval for monitoring large database in hour	Specify an interval in hours to detect and log MySQL database tables exceeding 10 GB. Range: One through 240 hours Default: One hour
Purge Health Data Older than in Month	Specify an interval in months to purge health-related data such as high CPU usage data in the **server.log** files. Range: One through 12 months Default: One month

14. (Optional) Click the **X509-Certificate-Parameters** hyperlink (on the left of the page) to add the X.509 certificate parameters that are validated during certificate parameter–based authentication.

    The right of the page displays the X.509 certificate parameters, as shown in Table 177.

    You can specify the parameters that are validated when a user logs in. The values for these parameters can be specified when you create the user in the Role Based Access Control workspace. For more information, see "Creating Users in Junos Space Network Management Platform" on page 1035.

    Table 177: X509 Certificate Parameter (Variable) Details

Column	Description
Comments	Comments about the X.509 certificate parameter Click the **view/configure** hyperlink to add comments.
Admin Status	Status of the parameter: active or inactive
Certificate Parameter	Name of the X.509 certificate parameter
Parameter Display Name	Description of the X.509 certificate parameter

    For more information about adding, deleting, modifying, and reordering the parameters, see "Adding and Activating X.509 Certificate Parameters for X.509 Certificate Parameter Authentication" on page 1451.

15. After you have modified the settings, you can do one of the following:

    - Save the changes by clicking the **Modify** button.

The Change Summary pop-up window displays the summary of the settings you modified. It also displays warnings, if any, regarding the changed settings. Click the **Confirm** button to save the changes. Alternatively, you can click the **Cancel** button to discard the modifications.

The settings that you modified are saved and you are taken back to the Applications page.

- Discard the changes by clicking the **Cancel** button.

  The changes you made are discarded and you are taken back to the Applications page.

For troubleshooting, see the **/var/log/jboss/servers/server1/server.log** file, which captures any internal errors, and the audit logs.

Release History Table

Release	Description
17.1R1	In each section of the Modify Application Settings (Modify Network Management Platform Settings) page, the settings that you modified are automatically saved from Junos Space Network Management Platform Release 17.1R1 onward.
17.1R1	From Release 17.1R1 onward, you can set a value of up to 480 minutes.
17.1R1	From Release 17.1R1 onward, you can override this setting by specifying a user-specific value when you create or modify a user account.
16.1R1	The **Disable inactive user after time period (Days)** setting is available from Release 16.1R1 onward.
16.1R1	The TLS 1.2 algorithm is available from Release 16.1R1 onward.

RELATED DOCUMENTATION

Modifying Settings of Junos Space Applications | **1345**

Worldwide Junos OS Adapter Overview | **371**

Systems of Record in Junos Space Overview | **214**

Creating Users in Junos Space Network Management Platform | **1035**

Managing File Integrity Check

IN THIS SECTION

- Configuring File Integrity Check | 1367
- Manually Checking File Integrity | 1368

The AIDE (Advanced Intrusion Detection Environment) file and directory integrity checker is supported in Junos Space Platform. AIDE enables you to take snapshots of all the configuration files, binaries, and library statistics and to find out the changes to files or binaries if a security breach occurs. From Release 17.2R1 onward, Junos Space Platform provides you an option to enable AIDE checks from the Junos Space Platform user interface.

When the file integrity check is enabled, Junos Space Platform takes a snapshot of the files in the system and checks the files for any modifications at specified intervals. Administrators are notified of changes to the files through SNMP traps.

When the file integrity check is enabled, Junos Space Platform shows the status of the file integrity check in the System Health Report in the Administration workspace. The **File Integrity Check Failed** item shows No or Yes values and provides a Click link to see the details. You can also manually do a file integrity check from the **Administration** > **Fabric** page by selecting a node and clicking the **Check for File Integrity** option in the right-click menu.

This topic explains the following tasks:

Configuring File Integrity Check

You can enable file integrity check and specify an interval for the file integrity check from the Junos Space Platform user interface.

To configure file integrity check:

1. From the Junos Space Platform user interface, go to **Administration** > **Applications**.

2. Select **Network Management Platform** and click **Modify Application Settings** from the **Actions** menu or the right-click menu.

   The Modify Network Management Platform Settings page appears.

3. Click **Health Monitoring** from the left pane.

The Health Monitoring page appears.

4. To enable file integrity check, select the **Enable File System Intrusion Detection Monitoring** check box.

   NOTE: You can edit the AIDE configuration file (**/etc/aide.conf**) from the Junos Space Platform CLI to modify the list of files or directories to monitor.

5. To specify the time interval at which Junos Space Platform should run file integrity check, enter a value (in hours) for **Interval for monitoring the File Changes in hours**.

   By default, **Interval for monitoring the File Changes in hours** is set to 24 hours.

6. Click **Modify** to save the settings. To discard the changes, click **Cancel**.

Manually Checking File Integrity

You can manually initiate a file integrity check from the Junos Space Platform user interface. From the AIDE File integrity results dialog box, you can review the changes and acknowledge the changes.

To manually initiate a file integrity check:

1. From the Junos Space Platform user interface, click **Administration** > **Fabric**.

2. Select the node for which you want to do the file integrity check and select **Check For File Integrity** from the **Actions** menu or the right-click menu.

   The AIDE File integrity results dialog box displays the file integrity check results including total number of files, added files, removed files, and changed files.

3. If you accept the changes, click **Acknowledge**. If you do not want to accept the changes, click **Close** to close the dialog box.

   Alternatively, click **Check Now** to rerun the file integrity check.

RELATED DOCUMENTATION

Modifying Junos Space Network Management Platform Settings | 1346

Starting, Stopping, and Restarting Services

This topic describes how to start, stop, and restart Network Monitoring (that is, the network monitoring services). Currently, Network Monitoring is the only service that can be managed this way.

Service management operations—start, stop, restart—are applied on all the nodes that run the service.

The service management actions generate audit log entries.

The Super Administrator and System Administrator predefined roles have the permissions to manage services; the corresponding action is Manage Services. If a user does not have a role that includes this action, the Manage Services option is not available.

The following table describes the consequences of performing these three actions:

Table 178: Starting, Stopping, and Restarting Network Monitoring

Action	Consequences
Stop	Network Monitoring service is stopped on all nodes.
	Even if VIP failover is performed, service remains stopped on all nodes.
	The synchronization of network monitoring data is disabled.
	Even after adding a new node, the network monitoring service remains stopped.
	Rebooting Junos Space Network Management Platform does not restart a service.
Start, **Restart**	Network Monitoring service starts only on the VIP node.
	All the devices displayed on the Devices page are discovered by the network monitoring functionality. The SNMP trap targets are correct.
	All the users displayed on the Users page are added to network monitoring.
	E-mail and remote server settings are added to network monitoring.
	All Junos Space nodes are monitored by the network monitoring functionality.
	The service continues to be operational even if Junos Space Network Management Platform is rebooted.
Start, Stop, Restart when no service is selected	An error message is displayed: No service selected.

NOTE: The following firewall ports should be closed on stopping the network monitoring service:

- UDP
  - 162
  - 514
  - 5813
- TCP
- 5813
- 18980

NOTE: Any devices added while the Network Monitoring service is stopped must be manually resynchronized from the Network Monitoring workspace after the service is restarted.

To start, stop, or restart network monitoring services:

1. Select **Administration** > **Applications**.

   The Applications inventory page appears.

2. Select **Network Management Platform** and select **Manage Services** from the Actions menu.

   The Manage Services page appears, showing the names of the services that can be managed this way (currently, Network Monitoring is the only item on this list), and the Start, Stop, and Restart buttons, as well as a table displaying the following information:

Column Heading	Content
Service Name	Name of service that can be started, stopped or restarted
Running Version	Version of the service that is currently running
Status	Current status: Enabled or Disabled

3. Select **Network Monitoring** from the list, and select the relevant button for a currently enabled service: **Start Service**, **Restart Service**, or **Stop Service**.

   One of four messages appears:

   - If you select a service that is currently running, then select **Stop Service**, you will receive this message:

```
Confirm Stop Service: Do you really want to stop the service?
```

- If you select a service that has been disabled, then select **Restart Service**, you will receive this message:

```
Warning: Sorry, cannot proceed with the request, as the Service is not
in Enabled state.
```

- If you select a service that has been disabled, then select **Start Service**, you will receive this message:

```
Warning: Sorry, Network Monitoring cannot be started once it is stopped.
```

- If you select a service that has been disabled, then select **Stop Service**, you will receive this message:

```
Warning: Sorry, cannot proceed with the request, as the Service is already
in Disabled state.
```

4. In all cases, you can click only **OK**.

   You first receive a message indicating that the relevant action is being performed. This is followed by a second status message indicating whether the operation you performed was successful or not.

5. Click **OK** to confirm.

   The Manage Services page reappears, displaying the changed status of the selected service.

RELATED DOCUMENTATION

- Managing Junos Space Applications Overview | 1328
- Managing and Unmanaging Interfaces and Services | 933
- Network Monitoring Workspace Overview | 799
- Junos Space Audit Logs Overview | 1115
- Role-Based Access Control Overview | 995

Adding a Junos Space Application

IN THIS SECTION

- Uploading the Junos Space Application | 1372
- Installing the Uploaded Junos Space Application | 1374

The administrator can add a new Junos Space application while Junos Space Network Management Platform is still running.

To upgrade Junos Space applications, see "Upgrading a Junos Space Application" on page 1376.

Adding an application to the Junos Space Platform server is a two-step process:

1. Upload the application to the Junos Space Platform server.

2. Install the uploaded application.

Uploading the Junos Space Application

To upload a Junos Space application:

1. Ensure that the Junos Space application you want to add is downloaded from the Juniper Networks software download site to the local client file system:

   https://www.juniper.net/support/products/space/#sw

2. Select **Administration** > **Applications** and click the Add Application icon.

   The Add Application page appears. If you have not uploaded any applications, the page is blank.

3. Upload the new application by performing one of the following steps:

   a. Click **Upload via HTTP**.

      The Software File dialog box appears.

      i. Type the name of the application file or click **Browse** to navigate to where the new Junos Space application file is located on the local file system.

      ii. Click **Upload**. This action might take a while. Wait until the application is uploaded.

If you are trying to upload an application that is not supported by Junos Space Platform 14.1R2, then Junos Space Platform displays the following error message:
Current platform version does not support this software version.

The Application Management Job Information dialog box appears. Go to step 4 to confirm whether the application is uploaded successfully.

b. Click **Upload via SCP**.

The Upload Software via SCP dialog box appears. Add the Secure Copy credentials to upload the Junos Space Platform application image from a remote server to Junos Space.

i. In the **Username** field, enter your username.

ii. In the **Password** field, enter your password.

iii. In the **Confirm password** field, enter your password again to confirm the password.

iv. In the **Machine IP** field, enter the host IP address.

> **NOTE:**
> - Depending on whether the Junos Space fabric is configured with only IPv4 addresses or both IPv4 and IPv6 addresses, Junos Space Platform allows you to enter an IPv4 address or either an IPv4 or IPv6 address respectively for the SCP server.
> - The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to http://www.iana.org/assignments/ipv4-address-space for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space for the list of restricted IPv6 addresses.

v. In the **Software File Path** field, enter the path name of the Junos Space application file.

For example, **/root/<*image-name*>.img**.

vi. Click **Upload**. This action might take a while. Wait until the application is uploaded.

If you are trying to upload an application that is not supported by Junos Space Platform Release 14.1R2, then Junos Space Platform displays the following error message:
Current platform version does not support this software version.

The Application Management Job Information dialog box appears. Go to step 4 to confirm whether the application is uploaded successfully.

4. In the Application Management Job Information dialog box, if you click the Job ID link, you see the Add Application job on the **Jobs > Job Management** inventory page. Wait until the job is completed and ensure that the job is successful.

   If the upload is successful, then the new application is displayed by application name, filename, version, release level, and the required Junos Space Platform version on the Add Application page.

Installing the Uploaded Junos Space Application

To install the uploaded application:

1. Select **Administration** > **Applications** and click the **Add Application** icon.

   The Add Application page appears.

2. Select the uploaded application.

3. Click **Install** to install the application or click **Cancel** to exit the Add Application page.

   The Application configuration page appears, displaying a list of server groups to which you can deploy the application.

   CAUTION: After you select and successfully deploy an application to a server group, it is not possible to move the application from one server group to another from the Junos Space GUI. So choose a server group after careful consideration. To move an application from one server group to another, use the script tool (see the instructions specified in "Running Applications in Separate Server Instances" on page 1338).

4. Select a server group to which you want to deploy the application.

   The default server group is **platform** to which Junos Space Platform is deployed. If you do not select any server group, the selected application is automatically deployed to the default **platform** server group.

5. Click **OK** to proceed.

   The Application Management Job Information dialog box appears.

6. In the Application Management Job Information dialog box, if you click the Job ID link, you see the Add Application job on the Job Management page. Wait until the application is fully deployed and ensure that the job is successful.

   If the installation of the application is a failure, then the Summary column for the installation job displays the reason for failure. However, the display of messages depends also on the type and version of the application being installed.

   > **NOTE:** It is important that you install the applications in the right order: from the primary application to the dependent applications.

7. If the installation is successful, without logging out of Junos Space Platform, select the application from the Application Chooser list (located at the top-left) to view and begin using its workspaces and tasks.

RELATED DOCUMENTATION

- Managing Junos Space Applications Overview | **1328**
- Managing Junos Space Applications | **1343**
- Junos Space Store Overview | **1333**
- Configuring and Managing Junos Space Store | **1334**
- Modifying Settings of Junos Space Applications | **1345**
- Uninstalling a Junos Space Application | **1406**

Upgrading a Junos Space Application

The Upgrade Application action allows you to upgrade an existing Junos Space application independently while the system is still running. Several hot-pluggable Junos Space applications are available for upgrade to the current release. After the application is upgraded successfully, you can launch it from Application Chooser.

> **CAUTION:** If you are upgrading a Junos Space application on a Junos Space Network Management Platform Release 16.1R1 setup, refer to the *Release Notes* for the specific Junos Space application release that you are upgrading to before you begin the upgrade process, to find out the specific upgrade instructions for the application release.

To upgrade an existing Junos Space application:

1. Download the application to which you want to upgrade from the Juniper Software download site to the local client file system.

   https://www.juniper.net/support/products/space/#sw

   > **CAUTION:** Do not modify the filename of the software image that you download from the Juniper Networks support site; if you modify the filename, the upgrade fails.

2. Select **Administration** > **Applications**. The Applications inventory page appears.

3. Select the application that you want to upgrade.

4. Select **Upgrade Application** from the Actions menu.

   The Upgrade Application dialog box appears displaying all previously uploaded versions of that application.

5. Do one of the following:

   - If the software file for the application to which you want to upgrade is listed in the Upgrade Application dialog box, select it and click **Upgrade**.

     The application upgrade process begins. Go to the next step.

- If the application to which you want to upgrade is not listed in the Upgrade Application dialog box, click **Upload**. The Software File dialog box appears.

a. Click **Browse** and navigate to where the software file to which you want to upgrade is located on the local file system.

b. Click **Upload**.

   The software file is uploaded into Junos Space Network Management Platform. You see the application in the Upgrade Applications dialog box.

c. Wait until the job is completed.

   The Upgrade Application Job Information dialog box appears.

d. Click the **Job ID** link to see the Upgrade Application job in the Manage Jobs inventory page. Review the job to:

   i. Ensure that the job is successful.

   ii. Select **Administration** > **Applications** to continue with the upgrade application process.

   The Upgrade Application dialog box appears.

e. Select the software file to which you want to upgrade, and click **Upgrade**. The application upgrade process begins.

6. Navigate to the Application Chooser and launch the application you upgraded.

   When you log into the application after the upgrade, an information dialog box with the following message is displayed: **Platform/Application is upgraded, please clear your browser cache and login again.**

   Click **OK** to close the information dialog box.

> **NOTE:** To install a new Junos Space application, use the **Administration** > **Applications** > **Add Application** action, see "Adding a Junos Space Application" on page 1372.

RELATED DOCUMENTATION

Managing Junos Space Applications Overview | **1328**

Managing Junos Space Applications | **1343**

Adding a Junos Space Application | 1372
Upgrading Junos Space Network Management Platform | 1378
Modifying Settings of Junos Space Applications | 1345
Uninstalling a Junos Space Application | 1406
Tagging an Object | 1526
Viewing Tags for a Managed Object | 1532

Upgrading Junos Space Network Management Platform

Junos Space Network Management Platform provides the running environment for all Junos Space applications, so upgrading causes operation interruption. The Upgrade Network Management Platform action allows the administrator to upgrade the Junos Space Platform independently from one version to another without installing other Junos Space applications.

NOTE:

- If you are upgrading to Junos Space Platform Release 16.1R1, you must follow the procedure outlined in Upgrading to Junos Space Network Management Platform Release 16.1R1.
- Refer to the *Upgrade Instructions* section in the *Junos Space Network Management Platform Release Notes* for a specific release to find out the versions of Junos Space Platform that are supported for upgrade.

NOTE: Before you upgrade Junos Space Platform to Release 17.2, ensure that the time on all Junos Space nodes is synchronized. For information about synchronizing time on Junos Space nodes, see “Synchronizing Time Across Junos Space Nodes” on page 1384.

To upgrade Junos Space Network Management Platform:

1. Ensure that the Junos Space Platform Upgrade image to which you want to upgrade is downloaded to the local client file system from the https://www.juniper.net/support/products/space/#sw website.

   CAUTION: Do not modify the filename of the software image that you download from the Juniper Networks support site. If you modify the filename, the upgrade fails.

2. Select **Administration** > **Applications**.

   The Applications page appears.

3. Right-click the **Network Management Platform** entry in the table and select **Upgrade Platform**. (Alternatively, select the **Network Management Platform** entry from the table and from the Actions menu, select **Upgrade Platform**.)

   The **Upgrade Platform** page appears displaying all previously uploaded versions of the Junos Space Platform image.

4. Do one of the following:

   - If the release to which you want to upgrade is listed on the Upgrade Platform page, select the file, and click **Upgrade**.

     The application upgrade process begins. (Go to step 8.)

   - If the release to which you want to upgrade is not listed on the Upgrade Platform page, you must upload the image file into Junos Space Platform. You can upload an image by using HTTP or Secure Copy Protocol (SCP):

     - To upload an image by using HTTP:

       a. Click **Upload via HTTP**.

          The Software File dialog box appears.

       b. Type the name of the Junos Space Platform image file or click **Browse** to navigate to where the new Junos Space Platform image file is located on the local file system.

       c. Click **Upload**.

> **CAUTION:** However, if the following error message appears, we recommend that you try uploading the image by using the **Upload via SCP** option: **File size is too big, use scp to upload this file**.

- To upload an image by using SCP:

  a. Click **Upload via SCP**.

     The Upload Software via SCP dialog box appears. You must add the following Secure Copy remote machine credentials.

  b. In the **Username** field, enter the username to be used to log in to the SCP server.

  c. In the **Password** field, enter the password to be used for access to the SCP server.

  d. In the **Confirm Password** field, reenter the password entered in the preceding step.

  e. In the **Machine IP** field, enter the IP address of the SCP server.

> **NOTE:**
> - Depending on whether the Junos Space fabric is configured with only IPv4 addresses or both IPv4 and IPv6 addresses, Junos Space Platform allows you to enter an IPv4 address or either an IPv4 or IPv6 address respectively for the SCP server.
> - The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to http://www.iana.org/assignments/ipv4-address-space for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space for the list of restricted IPv6 addresses.

  f. In the **Software File Path** field, enter the full path of the Junos Space Platform image file on the SCP server.

  g. Click **Upload**.

The new Junos Space Platform image file is uploaded into the Junos Space server and displayed by application name, filename, version, release type, and required Junos Space Platform version.

When the upload is completed, the Upgrade Platform Job Information dialog box appears.

5. In the Upgrade Platform Job Information dialog box, click the Job ID hyperlink.

You are taken to the Jobs Management page, where you can view the Upgrade Platform job that was triggered.

Ensure that the job is successful.

6. Select **Administration** > **Applications** to continue with the upgrade process.

   The Applications page appears.

7. Select the **Network Management Platform** entry from the table and from the Actions menu (or right-click menu) select **Upgrade Platform**.

   The **Upgrade Platform** page appears displaying the Junos Space Platform image that you uploaded.

8. Select the image file to which you want to upgrade, and click **Upgrade Platform**.

   NOTE:

   - If you have previously installed other Junos Space applications and if some applications are incompatible with the version of Junos Space Platform to which you are upgrading, an upgrade warning message appears informing you about the list of applications that might be disabled after the upgrade:

     a. Make a note of these applications and upgrade them after the Junos Space Platform upgrade is completed successfully.

     b. Click **OK** to close the dialog box.

   - Another upgrade warning message appears asking you whether you want the system to back up the database before the platform upgrade. Click **YES** or **NO** depending on whether you want the system to back up the Junos Space Platform database before the upgrade.

     Backing up the database before the upgrade helps you to recover the data if the platform upgrade fails. However, the upgrade process might be prolonged depending on the database size.

     When you choose to back up the database before the upgrade, you are directed to the "Database Backup and Restore" workspace. Follow the instructions specified in "Backing Up the Junos Space Network Management Platform Database" on page 1308 to back up the database.

     After backing up the database, select **Administration > Applications > Network Management Platform > Upgrade Platform > Upgrade** action to upgrade Junos Space Platform. When prompted for the second time, whether you want the system to back up the database, click **NO** to proceed with the upgrade.

Junos Space Platform goes into maintenance mode and prompts you to enter a username and password to enter maintenance mode and proceed with the upgrade.

9. In the **Username** field, enter the username (**maintenance**).

10. In the **Password** field, enter the maintenance mode password.

> **NOTE:** The maintenance mode password is one that the administrator created during the initial configuration process.

11. Click **OK**.

    The Junos Space Platform upgrade process begins. The Software Install Status dialog box appears and displays status messages using which you can monitor the upgrade status. The Upgrade Status Summary field in the Software Install Status dialog box displays additional information about the upgrade status. In addition, if any error occurs during the upgrade, information about the error or warning that led to the upgrade failure and the location of the log files for troubleshooting is displayed.

    This process might take a while. Wait until the **Go to Maintenance Menu** link appears.

12. Click the **Go to Maintenance Menu** hyperlink.

    The Maintenance Mode Options dialog box appears.

13. Click **Reboot Junos Space**.

    The installation progress dialog box appears and displays the deployment status of JBoss and various other applications as the system goes through a restart after the upgrade.

> **CAUTION:** This process might take a while. Do not reboot the system for a quick recovery. This action leaves the system in a bad state and affects the upgrade operation. Wait until the login window is presented for you to log in.

NOTE:

- During startup, the startup page first displays a message indicating that Junos Space Platform is starting up and then displays a progress bar indicating the percentage of startup completed, the estimated time left for the Junos Space Platform to start, and a list of tasks to complete (with an indication of the current task being carried out). When a task is successfully completed, a message is displayed; if a task fails, an error message is displayed indicating why the task failed.
- From Junos Space Network Management Platform Release 15.1R1 onward, a reboot message is broadcast to all the fabric nodes at the same time. All nodes reboot at the same time but the VIP node is the last to finish rebooting. The reboot procedure is significantly quicker than for previous Junos Space Platform releases.

When the upgrade is completed, the Junos Space login prompt appears.

NOTE:

- If a blank page appears instead of the login prompt, click Refresh. The login prompt is then displayed.
- We recommend that you clear the Web browser cache before logging in to the upgraded software.
- We recommend that you perform a functional audit on all deployed services after upgrading.

You can now log in to the upgraded Junos Space Platform software.

When you log into Junos Space Platform after the upgrade, an information dialog box with the following message is displayed: **Platform/Application is upgraded, please clear your browser cache and login again.**

Click **OK** to close the information dialog box.

For any troubleshooting, see the following logs:

- **/var/log/install.log**—This file captures information about the Junos Space Platform upgrade and the installation of applications.
- **/var/log/jboss/servers/server1/server.log**—This file captures information about JBoss.

RELATED DOCUMENTATION

Upgrading Junos Space Network Management Platform Overview | 1330

Managing Junos Space Applications Overview | 1328
Managing Junos Space Applications | 1343

Synchronizing Time Across Junos Space Nodes

Before you upgrade Junos Space Network Management Platform to Release 17.2, you must ensure that the time across all Junos Space nodes is synchronized.

To synchronize the system time across Junos Space nodes:

1. Log in to the Junos Space CLI.

   The Junos Space Settings Menu appears.

2. Type **3** and press Enter to access **Change Time Options** from the Junos Space Settings menu.

   The **Change Time Options** menu appears.

3. To access the **NTP options** to see whether an NTP server is configured, type **2** and press Enter.

   The **NTP options** menu appears.

   If an external NTP server is configured, the **NTP options** menu displays the domain name or IP Address of the NTP server along with the host name of other nodes in the cluster.

   If an external NTP server is not configured, the **NTP options** menu displays the host name of other nodes in the cluster.

4. Type **M** to access the Junos Space Settings menu.

   The Junos Space Settings menu appears.

5. To access the shell from the Junos Space Settings menu, type one of the following options:

   - **6**, if the Junos Space Appliance is a JA2500 Junos Space hardware appliance
   - **7**, if the Junos Space Appliance is a virtual appliance

   You are prompted to enter the administrator password.

6. Enter the administrator password.

7. Check whether the time is synchronized across nodes.

   If an external NTP server is configured, check whether the time on all Junos Space nodes is synchronized with the time on the NTP server.

   a. Check the time on the NTP server by entering the following command:

      ntpdate -q *NTPServerName*

      Here *NTPServerName* is the domain name or IP address of the NTP server.

      Press Enter.

      The time on the NTP server is displayed.

   b. Check the time on the Junos Space nodes by entering the following command on each node:

      date

      The time on the corresponding Junos Space node is displayed.

   If an external NTP server is not configured, check whether the time on all Junos Space nodes is synchronized with that on the VIP node.

   a. Check the time on the VIP node by entering the following command:

      date

      The time on the VIP node is displayed.

   b. Verify the time on non-VIP nodes by entering the following command on each node:

      date

      The time on the corresponding Junos Space node is displayed.

8. If the time on Junos Space nodes is not synchronized, execute one of the following procedures:

   If an external NTP server is configured, synchronize the time on all Junos Space nodes with that on the NTP server. To synchronize the time, execute the following procedure on all Junos Space nodes:

   a. Stop the NTP process by entering the following command:

      service ntpd stop

      The NTP process is stopped.

   b. Synchronize the time on the node by entering the following command:

      ntpdate -b *NTPServerName*

      Here *NTPServerName* is the domain name or IP address of the NTP server. The time on the Junos Space node is synchronized with that on the NTP server.

c. Restart the NTP process by entering the following command:

service ntpd start

The NTP process is restarted.

If an external NTP server is not configured, synchronize the time on all non-VIP nodes with that on the VIP node. To synchronize the time, execute the following procedure on all non-VIP nodes:

a. Stop the NTP process by entering the following command:

service ntpd stop

The NTP process is stopped.

b. Synchronize the time on the node by entering the following command:

ntpdate -b *VIPAddress*

Here *VIPAddress* is the Virtual IP (VIP) address of the Junos Space fabric. The time on the Junos Space node is synchronized with that on the VIP node.

c. Restart the NTP process by entering the following command:

service ntpd start

The NTP process is restarted.

The time on all Junos Space nodes is synchronized.

9. Set the time on the hardware clock to the system time by entering the following command:

hwclock --systohc

The time on the hardware clock is synchronized with that on the system.

The time across all Junos Space nodes is synchronized. You can now proceed to upgrading to Junos Space Platform Release 17.2.

RELATED DOCUMENTATION

Upgrading Junos Space Network Management Platform Overview | **1330**

Upgrading Junos Space Network Management Platform | **1378**

NTP Time Source for a Junos Space Appliance

Upgrading to Junos Space Network Management Platform Release 16.1R1

IN THIS SECTION

- Before You Begin | 1388
- Downloading and Installing the Junos Space Platform 15.2R2 Patch | 1389
- Executing the Data Back Up Procedure | 1390
- Validating the Backup File | 1394
- Installing Junos Space Platform Release 16.1R1 as a Standalone Node or the First Node of the Fabric and Restoring the Backed-Up Data | 1396
- Rolling Back to Junos Space Platform Release 15.2R2 if Upgrade Fails | 1399
- Installing Junos Space Platform Release 16.1R1 on the Remaining Nodes of the Fabric | 1403
- Configuring Device Communication | 1404
- Managing Disaster Recovery Configuration after Upgrade to 16.1 | 1405
- Appendix: Sample Data of Time Taken for Backup and Restore While Upgrading to Junos Space Platform Release 16.1R1 | 1405

In Junos Space Network Management Platform Release 16.1R1, CentOS 6.8 is used as the underlying OS. As a direct upgrade of the OS from CentOS 5.9 (used in Junos Space Platform releases before 16.1R1) to CentOS 6.8 is not supported, a direct upgrade to Junos Space Platform Release 16.1R1 by using the Junos Space Platform UI is also not supported. You must follow a multi-step procedure to upgrade to Junos Space Platform Release 16.1R1.

Upgrading to Junos Space Platform Release 16.1R1 involves backing up data from the nodes in the Junos Space Platform setup, installing Junos Space Platform Release 16.1R1 on the nodes, and restoring backed up data to the nodes. After Junos Space Platform is upgraded, you can upgrade previously installed Junos Space applications.

You can upgrade to Junos Space Platform Release 16.1R1 only from Junos Space Platform Release 15.2R2. To upgrade to Junos Space Platform Release 16.1R1 from releases earlier than Junos Space Platform Release 15.2R2, you must first upgrade to Junos Space Platform Release 15.2R2 and then follow the procedures specified in this topic.

NOTE: For more information about upgrading to Junos Space Platform Release 15.2R2, see the Junos Space Network Management Platform Release 15.2R2 Release Notes.

To upgrade from Junos Space Platform Release 15.2R2 to Junos Space Platform Release 16.1R1, complete the tasks in the sequence below. The Appendix provides sample data of time taken for backing up and restoring data while upgrading to Junos Space Platform Release 16.1R1.

Before You Begin

> **NOTE:** This particular upgrade procedure is complex and requires switching between the Junos Space Platform GUI and the Junos Space Platform command line. In case of problems, access to the physical appliance or the hypervisor that hosts the Junos Space virtual machine may be needed. If you are not comfortable running Linux commands at the command line, or you do not have access to the physical or virtual platform, the GUI, or the command line, please arrange for that access through the appropriate internal channels, and have the needed personnel available during the entire process.

Table 179 shows various physical and network elements that are needed in order to perform this upgrade procedure.

Table 179: Items needed for upgrade

Item	Purpose	Comments
Access to the Junos Space Platform GUI using the super user's credentials	To establish and confirm proper configuration, device connection, database state, and backup prior to upgrade	
Access to the Junos Space Platform command line using the admin user's credentials over SSH (TCP port 22)	To run various scripts and Linux commands during the upgrade	Once authenticated over ssh, select the "(Debug) run shell" option from the menu. On a physical appliance, (Debug) is option 6. On a virtual appliance, (Debug) is option 7.
Access to a network secure copy protocol (SCP) server	To store the following files that are created as part of the backup that is created during this upgrade: • backupStatus.log • md5.txt • space-15.2R2.4.tgz • space-readme.txt	SCP connections default to TCP port 22. Ports other than TCP port 22 can be used for SCP, but the server must already be set to accept the connection on the non-default port. Not needed if the USB storage device option is used.

Table 179: Items needed for upgrade *(continued)*

Item	Purpose	Comments
A USB storage device with at least 8GB of free space	To store the following files that are created as part of the backup that is created during this upgrade: • backupStatus.log • md5.txt • space-15.2R2.4.tgz • space-readme.txt	Not needed if the SCP option is used.
Physical access to the Junos Space Platform appliance	To plug in the USB storage device	Not needed if the SCP option is used.
Access to the hypervisor that hosts the Junos Space Platform VM	To deploy the 16.1R1 ova file	

Downloading and Installing the Junos Space Platform 15.2R2 Patch

Before you begin upgrading Junos Space Platform Release 15.2R2 to Junos Space Platform Release 16.1R1, download and install the Junos Space Platform Release 15.2R2 patch from the link *Junos Space 15.2R2 Backup Patch for Upgrade to 16.1R1 and 16.1R2* on the Junos Space Network Management Platform – Download Software page for *Version 16.1*.

To download and install the patch:

1. Download the 15.2R2 patch to your local computer from the *Junos Space 15.2R2 Backup Patch for Upgrade to 16.1R1 and 16.1R2* link at the following location:

   https://www.juniper.net/support/downloads/?p=space#sw

2. Log in to the Junos Space active VIP node as the admin user using SSH.

3. Transfer the patch to the Junos Space node by using Secure Copy Protocol (SCP).

   For example, to pull the file from the SCP server to a temporary location, such as **/tmp/patch** on the Junos Space node, the commands would be:

   Create the temporary storage location on the Junos Space node:

   ```
   [root@space-15.2R2-node ~]# mkdir /tmp/patch
   ```

Pull the file from the SCP server located at IP address 192.0.2.10:

```
[root@space-15.2R2-node ~]# scp user@192.0.2.10:/home/user/15.2R2.2-SpaceUpgradeBackup.tgz /tmp/patch
```

4. Navigate to the location on the Junos Space node where you stored the patch.

```
[root@space-15.2R2-node ~]# cd /tmp/patch
```

5. (Optional) To verify the checksum for the downloaded file, type the following command:

   [root@space-15.2R2-node /tmp/patch]# md5sum 15.2R2.2-SpaceUpgradeBackup.tgz

   The md5 hash value is displayed on the screen. Compare this value with the md5sum value available at the download site by clicking the MD5 SHA1 link.

6. Extract the patch by using the following command:

   [root@space-15.2R2-node /tmp/patch]# tar -xzvf 15.2R2.2-SpaceUpgradeBackup.tgz

   Extracting the patch creates a directory named **15.2R2.2-SpaceUpgradeBackup** and puts the individual files in it, including the patch script, **patchme.sh**.

7. Change directory into the new directory:

   [root@space-15.2R2-node /tmp/patch]# cd 15.2R2.2-SpaceUpgradeBackup

8. Type the following command to install the patch:

   [root@space-15.2R2-node /tmp/patch/15.2R2.2-SpaceUpgradeBackup]# sh patchme.sh

   If the patch is successful, the message “Hot Patch installed Successfully” will be displayed. Otherwise, errors will be displayed.

Executing the Data Back Up Procedure

To back up Junos Space Platform and Junos Space Application data from the Junos Space nodes, execute the backup script, **backup.sh** that is provided by the 15.2R2 patch that you installed. The **backup.sh** script is stored in the directory **/var/cache/space-backup-restore**.

The backup script backs up the required configuration files, data files, and the database dump files of the MySQL, PostgreSQL, and Cassandra databases from the Junos Space nodes. Data files of the installed Junos Space Applications are also backed up. The backup script generates a compressed tar file containing the backed up data. The following files are copied to a remote server or USB:

- space-15.2R2.4.tgz
- space-readme.txt
- md5.txt
- backupStatus.log

WARNING: In order for the upgrade process to succeed, the backup script must run to completion without errors. Read all warnings and notices generated by the backup script carefully and respond appropriately. Seek assistance for any message that is unclear to you before taking any action in response.

To run the backup script:

1. If you have not done so, log in to the Junos Space active virtual IP (VIP) node as the admin user and select “(Debug) run shell” from the menu.

2. Type the following command to navigate to the **/var/cache/space-backup-restore** directory:

   [root@space-15.2R2.2-node ~]# cd /var/cache/space-backup-restore

3. Type the following command to run the backup script:

   [root@space-15.2R2.2-node /var/cache/space-backup-restore]# sh backup.sh

   You are prompted to specify whether you want to clear system-related jobs from the Junos Space database.

4. Perform one of the following actions based on whether you want to clear system-related jobs or not:

   NOTE: Throughout the running of the **backup.sh** script, the responses that you type in the Space Platform command line may not be echoed to the screen. So, when you type ’Y’ or ’N’, you may not see it displayed.

   - Type **Y** to clear system-related jobs.
   - Type **N** if you do not want to clear system-related jobs.

     If you choose not to clear system-related jobs, the jobs are not purged and are backed up by the backup script.

   You are prompted to specify whether you want to stop the services running on the node.

5. Perform one of the following actions based on whether you want to continue backing up Junos Space data:

   - Type **N** to continue running the services on the node and exit the backup process.

     > **CAUTION:** If you exit the backup process, the backup file required for restoring data on the Junos Space Platform Release 16.1R1 setup is not generated.

   - Type **Y** to stop services running on the node and to continue the backup procedure.

     > **NOTE:** If you have Junos Space Service Now installed, you are prompted to confirm whether you want to restore the same version of the Service Now image that is currently installed, after the Junos Space Platform upgrade. Select the required option and follow the prompts that appear on the console. For more information, see the Junos Space Service Automation Release 16.1R1 release notes.
     >
     > If you are taking a backup of Service Now Release 16.2R1 installed on Junos Space Platform Release 15.2R2, follow the procedure, *Taking Back Up of Service Now Release 16.2R1 Data Before Upgrading Junos Space Platform to Release 16.1R1*, provided in the Service Now Release 16.2R1 release notes.

   You are prompted to select the location to store the generated backup files.

   ```
   1.USB
   2.Remote SCP server
   Option to Select :
   ```

6. Select one of the following options depending on where you want to store the backup files:

   - To store the files on a USB storage device:

     > **NOTE:** Before you back up to the USB storage device, you must ensure that the USB device is plugged in. The backup script will mount the device to the path **/tmp/pendrive**.

     a. Type **1** and press Enter.

        You are prompted to specify whether you want to continue.

     b. Type **Y** to continue. Table 179 These files are copied to the USB storage device.

If successful, a message indicating that the files are successfully copied is displayed. Any errors and their results are also displayed.

c. After successful copy we suggest that you validate the backup file. See "Validating the Backup File" on page 1394. If validation is successful, you can unmount the USB storage device by typing the following command:

[root@space-15.2R2.2-node /var/cache/space-backup-restore]# umount /tmp/pendrive. After this, you can unplug the USB device. However, if you are upgrading on the same appliance, we recommend leaving the USB storage device mounted and plugged in so that it is available later for the restore process.

- To store the file on a remote SCP server:

a. Type **2** and press Enter.

You are prompted to specify whether you want to continue.

Type **Y** to continue.

b. You are prompted to enter the IP address of the remote SCP server.

```
Please enter remote machine IP:
```

Type the IPv4 address of the remote SCP server.

c. You are prompted to enter the port number of the remote SCP server.

```
Please enter remote machine port number:
```

Type the port number of the remote SCP server and press Enter.

> **NOTE:** The IP address and port must be reachable from the Junos Space Platform server. If the IP is not reachable, or the port is not open, the script will get stuck trying to test the connection. If this happens, only quitting the SSH session, logging in again, and killing the running script process will stop the script.

d. You are prompted to enter the username to access the remote SCP server.

```
Please enter remote machine user:
```

Type the username and press Enter.

e. You are prompted to enter the password of the user.

```
Please enter remote machine user password:
```

Type the password and press Enter.

f. You are prompted to enter the full path of the directory on the remote SCP server where you want to store the backup files.

```
Please enter remote dir path:
```

Type the full path of the directory and press Enter.

For example, **/home/user/space_backup/**

> **NOTE:** Ensure that there is no space character in the specified directory path. Also, ensure that the specified directory already exists on the remote SCP server. If the directory does not exist, you are prompted to enter a valid directory.

Table 179

Validating the Backup File

After executing the data backup procedure, we recommend that you validate the checksum for the backup file to ensure that the data from the Junos Space Platform Release 15.2R2 setup is copied to the selected backup location. This ensures that data from the Junos Space nodes is not lost and can be restored on the Junos Space Platform Release 16.1R1 setup when you upgrade.

To validate the backup file, complete one of the following procedures:

- To validate the backup file stored on a remote SCP server:

1. Log in to the remote SCP server.
2. Navigate to the directory where the backup file is stored.
3. Type the following command and press Enter to generate the MD5 value for the backup file:

[user@scp-server]> md5sum space-15.2R2.4.tgz

> **NOTE:** On some systems, there is no md5sum command. On these systems, the **md5 *<file name>*** command should print the md5 hash value.

4. Compare the calculated MD5 value with the value in the **md5.txt** file stored at the same location as the backup file. You can see the value stored in **md5.txt** using the following command:

   [user@scp-server]> cat md5.txt

   If the MD5 values are the same, the backup file is copied successfully to the backup location. If the MD5 values do not match, repeat the back up procedure detailed in "Executing the Data Back Up Procedure" on page 1390.

5. You can verify the integrity of the backup tar file to ensure that errors did not result in a corrupt backup file. To do this, type the following command and press Enter to verify the files in the backup tar file:

   [user@scp-server]> tar -tf space-15.2R2.4.tgz

   The list of files contained in the tar file are displayed. If there are errors in the tar file, the error is displayed and the file listing stops.

- To validate the backup file stored on a USB storage device:

  > **NOTE:** Ensure that the USB storage device is plugged-in to the Junos Space Appliance and mounted to the path **/tmp/pendrive**.

  1. Type the following command and press Enter to generate the MD5 value for the backup file:

     [root@space-15.2R2-node ~]# md5sum /tmp/pendrive/space-15.2R2.4.tgz

  2. Compare the calculated MD5 value with the value in the **md5.txt** file stored at the same location as the backup file. You can see the value stored in **md5.txt** using the following command:

     [root@space-15.2R2-node]# cat md5.txt]

     If the MD5 values are the same, the backup file is copied successfully to the backup location. If the MD5 values do not match, repeat the back up procedure detailed in "Executing the Data Back Up Procedure" on page 1390.

  3. Type the following command and press Enter to verify the files in the backup tar file:

     [root@space-15.2R2-node]# tar -tf /tmp/pendrive/space-15.2R2.4.tgz

The list of files contained in the tar file are displayed. If there are errors in the tar file, the error is displayed and the file listing stops.

Installing Junos Space Platform Release 16.1R1 as a Standalone Node or the First Node of the Fabric and Restoring the Backed-Up Data

After you run the backup script and back up data from the Junos Space nodes, install the Junos Space Platform Release 16.1R1 software image, using the following procedure:

CAUTION:

- If you are upgrading a standalone node, back up all data on the node to a remote server before you install the Junos Space Platform Release 16.1R1 software image. You cannot retrieve previously saved data after the Junos Space Platform Release 16.1R1 software image is installed.
- When you configure the Junos Space Platform Release 16.1R1 node, ensure that you use the same network configuration (network interfaces and IP adresses) as the Junos Space Platform Release 15.2R2 node. If you configure different network settings, device connectivity and SNMP traps are affected.

1. Power off all the nodes of the fabric.

   NOTE: If you are upgrading a Junos Space Platform fabric with only Junos Space Virtual Appliances, ensure that you do not delete the powered off virtual appliances. If data restore on the Junos Space Platform Release 16.1R1 node fails, you can roll back to the Junos Space Platform Release 15.2R2 setup by powering off the Junos Space Platform Release 16.1R1 node and powering on the Junos Space Platform Release 15.2R2 nodes.

2. Complete one of the following procedures:

   - If the Junos Space Platform fabric has only Junos Space Appliances (JA2500 or JA1500), power on one of the appliances that is part of the fabric and reimage it by following the procedure in 3.

> **CAUTION:** If you are upgrading a Junos Space Platform setup with a single Junos Space Appliance (JA2500 or JA1500), you must validate the backup file before you reimage the appliance with the Junos Space Platform Release 16.1R1 software image. If you do not ensure that the data backup from the Junos Space Platform Release 15.2R2 setup is complete before you reimage the appliance, the data is lost. For information about validating the backup file, see "Validating the Backup File" on page 1394.

- If the Junos Space Platform fabric has Junos Space Virtual Appliances, deploy a new Junos Space Platform Release 16.1R1 virtual appliance instance and configure it as a Junos Space node by following the procedure in 3.

3. Install Junos Space Platform Release 16.1R1 and restore data by using one of the following procedures:

   > **NOTE:** To ensure that you upgrade Junos Space Platform and not choose a fresh installation of Junos Space Platform Release 16.1R1, select the option to restore backed-up data when you are prompted during the configuration of the node.

   - To deploy and configure the Junos Space Virtual Appliance, see the Deploying the Junos Space Virtual Appliance and Configuring a Junos Space Virtual Appliance as a Junos Space Node topics in the Junos Space Virtual Appliance Installation and Configuration Guide.
   - To install and configure the Junos Space Platform Release 16.1R1 software image on a JA2500 Junos Space Appliance, see the Installing a Junos Space Image on a Junos Space Appliance by Using a USB Drive and Configuring a Junos Space Appliance as a Junos Space Node topics in the JA2500 Junos Space Appliance Hardware Guide.
   - To install and configure the Junos Space Platform Release 16.1R1 software image on a JA1500 Junos Space Appliance, see the Installing a Junos Space Image on a Junos Space Appliance by Using a USB Drive and Configuring a Junos Space Appliance as a Junos Space Node topics in the JA1500 Junos Space Appliance Hardware Guide.

   If the messages displayed on the console indicate that data is restored successfully and JBoss services are started on the node, you can access the Junos Space Platform GUI through a browser by using the virtual IP (VIP) address configured for Web access.

4. (Optional) If the messages displayed on the console indicate that data is not restored successfully, you can roll back to the Junos Space Platform Release 15.2R2 setup. See "Rolling Back to Junos Space Platform Release 15.2R2 if Upgrade Fails" on page 1399.

5. If the Junos Space Platform Release 15.2R2 setup had Junos Space applications installed, after the data is restored successfully and the Junos Space Platform GUI becomes accessible, you must upgrade the applications to releases that are compatible with Junos Space Platform Release 16.1R1 by using the Junos Space Platform GUI.

   > **NOTE:** After the upgrade to Junos Space Platform Release 16.1R1, the Junos Space applications that were installed prior to the upgrade, with the exception of Junos Space Service Now Releases 15.1R3, 15.1R4, and 16.1R1, appear disabled. For more information about upgrading an application, refer to the release notes of the Junos Space application that you want to upgrade.

   Before you install or upgrade an application, verify the DNS server configuration.

   To ensure that the DNS server is configured correctly:

   a. Log in to the Junos Space command line as the admin user.

      The Junos Space Settings Menu appears.

   b. On the Junos Space Settings Menu, to access the shell, type the number corresponding to "(Debug) run shell".

      On a Junos Space Appliance, "(Debug) run shell" is number 6.

      On a Junos Space Virtual Appliance, "(Debug) run shell" is number 7.

      You are prompted to enter the administrator password.

   c. Enter the administrator password.

   d. Type the following command at the command prompt and press Enter:

      [root@space-16.1R1-node ~]# host -a localhost

      If the output of the command contains the following line, or if the output contains the IPv4 address as well as the IPv6 address, you must modify the DNS server configuration in Junos Space Platform:

      localhost. 86400 IN AAAA ::1

      To modify the DNS server configuration, go to step e, else, go to step f.

   e. To modify the DNS server configuration in Junos Space:

      i. Type the following command to create a backup of the **resolv.conf** file:

         [root@space-16.1R1-node ~]# cp /etc/resolv.conf /etc/resolv.conf.orig

ii. Delete all entries in the **resolv.conf** file with the following command:

[root@space-16.1R1-node ~]# echo “”/etc/resolv.conf

f. Install or upgrade the required Junos Space applications from the Junos Space Platform GUI.

For more information, see the release notes of the Junos Space application that you want to install or upgrade.

g. If you modified the DNS server configuration before installing or upgrading the applications, type the following command to revert to the original configuration, after you have installed or upgraded all required applications:

[root@space-16.1R1-node ~]# cp /etc/resolv.conf.orig /etc/resolv.conf

Type y and press Enter when asked if you want to overwrite **/etc/resolv.conf**.

6. After you have verified that the data is restored successfully, if the node you upgraded is the first node of a Junos Space fabric, install the Junos Space Platform Release 16.1R1 software image on the remaining nodes of the fabric. See “Installing Junos Space Platform Release 16.1R1 on the Remaining Nodes of the Fabric” on page 1403.

Rolling Back to Junos Space Platform Release 15.2R2 if Upgrade Fails

While upgrading to Junos Space Platform Release 16.1R1, if you are unable to restore the data backed up before you began upgrading Junos Space Platform, you can roll back to Junos Space Platform Release 15.2R2.

If data restore fails, complete one of the following procedures:

- If the Junos Space node is a standalone node:

1. Complete one of the following procedures:

   - For a Junos Space Appliance (JA2500 or JA1500), reimage the node to install the Junos Space Platform Release 15.2R2 software image, by using one of the following procedures:

     - To install and configure the Junos Space Platform Release 15.2R2 software image on a JA2500 Junos Space Appliance, see the Installing a Junos Space Image on a Junos Space Appliance by Using a USB Drive and Configuring a Junos Space Appliance as a Junos Space Node topics in the JA2500 Junos Space Appliance Hardware Guide.

     - To install and configure the Junos Space Platform Release 15.2R2 software image on a JA1500 Junos Space Appliance, see the Installing a Junos Space Image on a Junos Space Appliance by Using a USB Drive and Configuring a Junos Space Appliance as a Junos Space Node topics in the JA1500 Junos Space Appliance Hardware Guide.

   - For a Junos Space Virtual Appliance, roll back to the Junos Space Platform Release 15.2R2 setup by powering off the Junos Space Platform Release 16.1R1 node and powering on the Junos Space Platform Release 15.2R2 node.

     The roll back of the Junos Space Virtual Appliance to Release 15.2R2 is complete.

2. Download and apply the Junos Space Platform Release 15.2R2 patch. See "Downloading and Installing the Junos Space Platform 15.2R2 Patch" on page 1389 to install the patch.

3. Install the same Junos Space applications that were installed on the Junos Space Platform Release 15.2R2 setup that you attempted to upgrade.

4. Type the following command to navigate to the **/var/cache/space-backup-restore** directory:

   [root@space-15.2R2-node ~]# cd /var/cache/space-backup-restore

5. Type the following command to restore the backup:

   [root@space-15.2R2-node /var/cache/space-backup-restore]# sh restore-15.2r2.sh

   You are prompted to specify the location from where you want to restore the backup.

```
1> Remote Server
2> USB
3> Local

M> Return to Main Menu
R> Redraw Menu

Choice [1-3 MR]:
```

6. Select one of the following options depending on where the backup file is stored:
   - To restore from a remote Secure Copy Protocol (SCP) server:
     a. Type **1** and press Enter.

        You are prompted to confirm whether you want to continue.

        ```
        You have selected [ Remote Server ]. Do you want to Continue? [Y/N]
        ```

     b. Based on whether you want to continue or exit, perform one of the following actions:
        - Type **Y**.

          You are prompted to enter the IPv4 address of the remote SCP server.

          ```
          Please enter Remote Server IP:
          ```

          i. Type the IPv4 address of the remote SCP server and press Enter.

             You are prompted to enter the port number for the remote server.

             ```
             Please enter port number for Remote Server REMOTE_SERVER_IP:
             ```

          ii. Type the port number of the remote SCP server and press Enter.

              You are prompted to enter the username to access the remote server.

              ```
              Please enter Remote Server REMOTE_SERVER_IP user:
              ```

          iii. Type the username and press Enter.

               You are prompted to enter the password of the user.

               ```
               Please enter Remote Server user REMOTE_SERVER_USER password:
               ```

          iv. Type the password and press Enter.

              You are prompted to enter the full path of the directory where the backup file is stored.

              ```
              Enter the path of the directory containing backup files:
              ```

          v. Type the full path of the directory and press Enter.

> **NOTE:** Ensure that the directory path does not contain any space characters.

The messages displayed on the console indicate whether the data is restored successfully to the Junos Space node.

- Type **N** to exit.

- To restore from a USB storage device:

> **NOTE:**
> - Before you restore from a USB storage device, ensure that the USB device is plugged in. The restore procedure will try to mount the device to the path **/tmp/pendrive**.
> - For data backup and restore, identify the USB storage device using the **fdisk -l** command and format the device using the **mkfs.ext2 <physical device>** command. For example, **mkfs.ext2 /dev/sdb**. This ensures that the USB device has the correct disk layout for the execution of the backup and restore procedures and prevents loss of data.

a. Type **2** and press Enter to restore the backup from the USB storage device.

   The messages displayed on the console indicate whether the data is restored successfully to the Junos Space node.

b. Unmount the USB storage device by typing the following command:

   [root@space-15.2R2-node /var/cache/space-backup-restore]# umount /tmp/pendrive

   You can unplug the USB storage device after you unmount it.

- To restore data from the backup file stored on the Junos Space node:

> **NOTE:** To restore data from the backup file stored on the Junos Space node, you must first copy the file from the backup location to the Junos Space node.

a. Type **3** and press Enter.

   You are prompted to enter the full path of the directory where the backup file is stored.

```
Enter the tar file path to restore from local:
```

b. Type the full path of the directory and press Enter.

The messages displayed on the node indicate whether the data is restored successfully to the Junos Space node.

If the messages displayed on the console indicate that the data is restored successfully and JBoss services are started on the node, you can access the Junos Space Platform UI through a browser by using the VIP address configured for Web access. You can now use this Junos Space Platform Release 15.2R2 installation.

If the restore fails, save the troubleshooting log file, **/var/log/restoreStatus.log** to your computer; power off the node; and contact Juniper Networks support for assistance.

- If the node is a Junos Space Appliance (JA2500 or JA1500) and the first node of a Junos Space fabric, complete the following procedure:

1. Power off the node.

2. Power on the remaining nodes of the cluster, to bring up the cluster with the Junos Space Platform Release 15.2R2 installation.

3. Delete the first node (on which upgrade failed) from the cluster, using the Junos Space Platform GUI. For more information about deleting the node, see "Deleting a Node from the Junos Space Fabric" on page 1259.

4. Power on and reimage the node that you attempted to upgrade, to install the Junos Space Platform Release 15.2R2 software image. To reimage the node, follow one of the procedures listed in 1.

5. Add the node to the fabric by using the Junos Space Platform GUI. For information about adding nodes to the Junos Space fabric, see "Adding a Node to an Existing Junos Space Fabric" on page 1176.

Installing Junos Space Platform Release 16.1R1 on the Remaining Nodes of the Fabric

When you upgrade from Junos Space Platform Release 15.2R2 to Junos Space Platform Release 16.1R1, if you have dedicated database nodes or Fault Monitoring and Performance Monitoring (FMPM) nodes configured for the Junos Space Platform setup that you are upgrading, after the upgrade and data restoration on the first node of the Junos Space fabric is complete, you must add the dedicated database nodes and FMPM nodes to the fabric by using the Junos Space Platform GUI. You can configure the nodes as Junos Space nodes or Fault Monitoring and Performance Monitoring (FMPM) nodes, by using one of the following procedures:

> **NOTE:** After you configure the nodes from the Junos Space Platform command line, you can add the nodes to the Junos Space fabric as JBoss nodes, dedicated database nodes, dedicated Cassandra nodes or FMPM nodes, by using the Junos Space Platform UI. For information about adding nodes to the Junos Space fabric, see "Adding a Node to an Existing Junos Space Fabric" on page 1176.

- To install and configure the Junos Space Platform Release 16.1R1 software image on a Junos Space Virtual Appliance, see the Deploying the Junos Space Virtual Appliance, Configuring a Junos Space Virtual Appliance as a Junos Space Node and Configuring a Junos Space Virtual Appliance as a Standalone or Primary FMPM Node topics in the Junos Space Virtual Appliance Installation and Configuration Guide.
- To install and configure the Junos Space Platform Release 16.1R1 software image on a JA2500 Junos Space Appliance, see the Installing a Junos Space Image on a Junos Space Appliance by Using a USB Drive, Configuring a Junos Space Appliance as a Junos Space Node, and Configuring a Junos Space Appliance as a Standalone or Primary FMPM Node topics in the JA2500 Junos Space Appliance Hardware Guide.
- To install and configure the Junos Space Platform Release 16.1R1 software image on a JA1500 Junos Space Appliance, see the Installing a Junos Space Image on a Junos Space Appliance by Using a USB Drive, Configuring a Junos Space Appliance as a Junos Space Node, and Configuring a Junos Space Appliance as a Standalone or Primary FMPM Node topics in the JA1500 Junos Space Appliance Hardware Guide.

Configuring Device Communication

After you upgrade to the Junos Space Platform Release 16.1R1, you must configure device communication to ensure that discovered devices can communicate with the Junos Space server.

To configure device communication:

1. On the Junos Space Platform GUI, select **Administration** > **Applications**.

   The Applications page is displayed.

2. Click **Network Management Platform** and select **Modify Application Settings** from the Actions menu. Alternatively, right-click **Network Management Platform** and select **Modify Application Settings**.

   The Modify Application Settings (Modify Network Management Platform Settings) page is displayed and the Device section is selected by default.

3. Select the **Allow Device Communication** check box.

4. Click **Modify** to modify the settings.

Devices discovered in Junos Space Platform can now communicate with the Junos Space server.

Managing Disaster Recovery Configuration after Upgrade to 16.1

If you have disaster recovery configured for the Junos Space Platform Release 15.2R2 setup that you are upgrading, you must upgrade both the active and standby sites to Junos Space Platform Release 16.1R2 as explained in this topic and then reconfigure disaster recovery. For information about configuring disaster recovery, see Configuring the Disaster Recovery Process Between an Active and a Standby Site.

Appendix: Sample Data of Time Taken for Backup and Restore While Upgrading to Junos Space Platform Release 16.1R1

In Table 180, you can view data gathered from test setups, which show the approximate time taken for data backup and restore while upgrading to Junos Space Platform Release 16.1R1.

Table 180: Sample Data Showing Approximate Time Taken for Backup and Restore

Database	CPU	CPU Speed MHz	RAM (GB)	Disk (GB)	Applications Installed	Backup Size (GB)	Backup Duration (HH:MM:SS)	Restore Duration (HH:MM:SS)
Database1	4	2500	32	140	Security Director, Service Now	5	0:23:34	0:44:14
Database2	4	2500	32	140	Service Now	15	0:53:45	1:35:40
Database3	4	2500	32	140	Service Now	3	0:21:27	0:19:41
Database4	4	2500	32	140	Security Director	2.6	0:27:00	0:22:56
Database5	4	2500	32	140	ICEAA	11	0:36:09	0:48:58
Database6	4	2500	32	140	None	2.7	0:24:00	1:04:54

RELATED DOCUMENTATION

Upgrading Junos Space Network Management Platform Overview | 1330

Uninstalling a Junos Space Application

The Uninstall application action allows the administrator to remove a Junos Space application independently while the system is still running. Uninstalling an application cleans up all database data and any process the application used. You can uninstall a Junos Space application from the Applications inventory page.

To uninstall a Junos Space application:

1. Select **Administration** > **Applications**.

   The Applications inventory page appears.

2. Select the application you want to uninstall and select **Uninstall Application** from the Actions menu.

   The Uninstall Application dialog box appears.

3. Select the application to confirm that you want to uninstall.

4. Click **Uninstall**.

   The application uninstall process begins and the Junos Space application is removed from Junos Space Network Management Platform. The association between the uninstalled application and the server group from which it was uninstalled is lost. The server group itself is not removed by the uninstallation of an application. However, if you want to delete the server group along with the application, use the JBoss Management CLI (see "Running Applications in Separate Server Instances" on page 1338).

> **NOTE:** It is important that you uninstall the applications in the right order: from the dependent applications to the primary application. The uninstallation might fail if there are any dependent applications.
>
> For example, if you try to uninstall Network Activate without uninstalling dependent applications, such as Transport Activate or OAM Insight, the following error message is displayed and the uninstallation fails: .
>
> **Network Activate Uninstall failed! Details: Uninstalling Network Activate is not possible until the dependency apps are uninstalled first Transport Activate, OAM Insight, Sync Design & NWappsAPI**
>
> The display of such messages depends on the type and version of the application being uninstalled.

RELATED DOCUMENTATION

Managing Junos Space Applications Overview | 1328

Modifying Settings of Junos Space Applications | 1345

Upgrading a Junos Space Application | 1376

Upgrading Junos Space Network Management Platform | 1378

CHAPTER 73

Managing Troubleshooting Log Files

IN THIS CHAPTER

- System Status Log File Overview | **1408**
- Customizing Node System Status Log Checking | **1410**
- Customizing Node Log Files to Download | **1412**
- Configuring JBoss and OpenNMS Logs in Junos Space | **1412**
- Generating JBoss Thread Dump for Junos Space Nodes | **1414**
- Downloading the Troubleshooting Log File in Server Mode | **1417**
- Downloading the Troubleshooting Log File in Maintenance Mode | **1420**
- Downloading Troubleshooting System Log Files Through the Junos Space CLI | **1421**

System Status Log File Overview

The system writes a system log file for each fabric node to provide troubleshooting and monitoring information. See "System Status Log File" on page 1408.

The System Administrator can customize the information that is collected in the system log file. See "Customizing Node System Status Log Checking" on page 1410.

The System Administrator can download the latest log files for each fabric node when logged in to a Junos Space Appliance. See "Downloading System Log Files for a Junos Space Appliance" on page 1409.

In each operating mode, the System Administrator can customize the default log files that are downloaded from a Junos Space Appliance. See "Customizing Node Log Files to Download" on page 1412.

System Status Log File

Approximately once a minute, the system checks and writes a status log file **SystemStatusLog** for each fabric node by default. Each log file consists of system status, such as the disk, CPU, and memory usage information, as shown. Junos Space Network Management Platform writes each system status log file to **/var/log/SystemStatusLog**

```
2009-08-10 11:51:48,673 DEBUG [net.juniper.jmp.cmp.nma.NMAResponse] (Thread-110:)
Node IP: 192.0.2.0Filesystem           1K-blocks      Used Available Use% Mounted
on
/dev/mapper/VolGroup00-LogVol00
                      79162184  15234764  59841252  21% /
Cpu(s):  8.7%us,  1.1%sy,  0.0%ni, 90.0%id,  0.1%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   3866536k total,  2624680k used,  1241856k free,    35368k buffers
Swap:  2031608k total,   941312k used,  1090296k free,   439704k cached
```

Customizing Status Log File Content

The System Administrator can customize the information that is written in a fabric node system status log file. For more information, see "Customizing Node System Status Log Checking" on page 1410.

Downloading System Log Files for a Junos Space Appliance

The System Administrator can download the latest log files for each fabric node when logged in to a Junos Space Appliance. The system status log file and all other third-party log files are collected and compressed in a troubleshooting file.

Table 181 lists the files included in the **troubleshoot** file.

Table 181: Log Files included in the troubleshoot File

Description	Location
System status log files	**/var/log/SystemStatusLog**
JBoss log files	**/var/log/jboss/***
Service-provisioning data files	**/var/tmp/jboss/debug/***
MySQL error log files	**/var/log/mysqld.log**
Log files for Apache, Node Management Agent (NMA), and Webproxy	**/var/log/httpd/***
Watchdog log files	**/var/log/watchdog/***
System messages	**/var/log/messages/***

The System Administrator can download log files in each operation mode as follows:

- Server mode (See "Downloading the Troubleshooting Log File in Server Mode" on page 1417.)
- Maintenance mode (See "Downloading the Troubleshooting Log File in Maintenance Mode" on page 1420.)

- CLI mode (See “Downloading Troubleshooting System Log Files Through the Junos Space CLI” on page 1421.)

Customizing Log Files to Download

The System Administrator can also customize the log files to be downloaded for specific fabric nodes. For more information about customizing node log files to download, see “Customizing Node Log Files to Download” on page 1412.

RELATED DOCUMENTATION

Customizing Node System Status Log Checking | **1410**

Customizing Node Log Files to Download | **1412**

Downloading the Troubleshooting Log File in Server Mode | **1417**

Downloading the Troubleshooting Log File in Maintenance Mode | **1420**

Downloading Troubleshooting System Log Files Through the Junos Space CLI | **1421**

Customizing Node System Status Log Checking

You customize the system status checking for a fabric node to ensure that all necessary information is written to the **/var/log/SystemStatusLog** log file. You must have the privileges of a System Administrator to customize the system status checking. You customize the system status checking by modifying the fabric node Perl script in **/usr/nma/bin/writeLogCronJob**.

To customize system status checking for a fabric node, modify the **writeSystemStatusLogFile** sub-function in **writeLogCronJob** as shown:

```
sub writeSystemStatusLogFile{
 my $err = 0;
my $logfile = $_[0];
$err = system("date >> $logfile");
$err = system("df /var >> $logfile");
$err = system("top -n 1 -b | grep Cpu >> $logfile");
$err = system("top -n 1 -b | grep Mem: >> $logfile");
$err = system("top -n 1 -b | grep Swap: >> $logfile");

***<Add additional system command here that you want to print out in the
SystemStatusLog file>***

 if ($err == 0 ) {                print "write log to $logfile successfully\n";

 } else {                print "cannot write log to $logfile\n";
 }
return $err;
 }
```

RELATED DOCUMENTATION

- System Status Log File Overview | **1408**
- Customizing Node Log Files to Download | **1412**
- Downloading the Troubleshooting Log File in Server Mode | **1417**
- Downloading the Troubleshooting Log File in Maintenance Mode | **1420**
- Downloading Troubleshooting System Log Files Through the Junos Space CLI | **1421**

Customizing Node Log Files to Download

You customize the log files downloaded for a fabric node to ensure that you download all the necessary log files. You must have the privileges of a System Administrator to customize the log files. You customize the log files you want to download by modifying the Perl script in **/var/www/cgi-bin/getLogFiles**.

Modify the **getLogFiles** Perl script zip command as shown:

```
. . .
system("zip –r $logFileName /var/log/jboss/* /var/tmp/jboss/debug/ /var/log/mysqld.log
 /var/log/httpd/* /var/log/watchdog /var/log/messages /var/log/SystemStatusLog >
/dev/null");
. . .
```

RELATED DOCUMENTATION

- System Status Log File Overview | **1408**
- Customizing Node System Status Log Checking | **1410**
- Downloading the Troubleshooting Log File in Server Mode | **1417**
- Downloading the Troubleshooting Log File in Maintenance Mode | **1420**
- Downloading Troubleshooting System Log Files Through the Junos Space CLI | **1421**

Configuring JBoss and OpenNMS Logs in Junos Space

From Junos Space Network Management Platform Release 16.1R1 onward, you can configure log levels for JBoss and OpenNMS logs in Junos Space from the Administration workspace in the Junos Space Platform UI. Junos Space Platform enables you to configure log levels for the JBoss and OpenNMS logs by using the Log Configuration page of the Space Troubleshooting task group. When you configure a particular log level, log messages for the selected severity and all higher severities are recorded.

You must be assigned the System Administrator role to configure logs from the Log Configuration page.

To configure the JBoss and OpenNMS logs from the Junos Space Platform UI:

1. On the Junos Space Platform UI, select **Administration** > **Space Troubleshooting** > **Log Configuration**.

   The Log Configuration page is displayed.

2. Perform one of the following actions to configure the JBoss or OpenNMS logs, respectively:

- Click the **JBoss Logs** tab.

  The log handlers configured in JBoss are listed on the page. The corresponding log filenames and log levels are also displayed in a tabular format. The Log Level column displays the existing log level for each log.

- Click the **OpenNMS Logs** tab.

  The log handlers configured in OpenNMS are listed on the page. The corresponding log filenames and log levels are also displayed in a tabular format. The Log Level column displays the existing log level for each log.

For more information about log files in Junos Space Platform, see "Junos Space Network Management Platform Log Files Overview" on page 1591.

3. Click the **Log Level** field of the log file for which you want to configure the log level.

4. Click the down arrow to select the log level from the list.

   When you select a particular log level, log messages for the selected severity and all higher severities are recorded. For example, if you select DEBUG as the log level, log messages for severity **DEBUG**, **INFO**, **WARN**, and **FATAL** are recorded in the log file for which you configured the log level. If you select ALL, all log messages are recorded in the log file. See Table 182 for more information about the log levels that you can select.

5. Click **Update** to save the change.

   Repeat Step 2 through Step 5 to modify log levels for other JBoss and OpenNMS logs listed on the page.

6. (Optional) Select or clear the check box in the **Enable/Disable** column to enable or disable logging for the corresponding log file. By default, logging for all JBoss and OpenNMS log files is enabled, unless it is disabled from the Junos Space CLI, and the default log level is WARN.

   If you select the check box, logging is enabled and the log level is set at the WARN level.

7. Click **Save** to save all changes after you finish specifying the log levels.

An audit log entry is added when you modify the log level of any log file.

Table 182 lists the various log levels that can be configured for JBoss and OpenNMS logs.

Table 182: Log Levels and their Descriptions

Log Level	Description
OFF	Logging is turned off.

Table 182: Log Levels and their Descriptions *(continued)*

Log Level	Description
FATAL	Log messages that indicate a critical service failure are recorded.
ERROR	Log messages that indicate a disruption in a request or the ability to service a request and all higher-severity log messages are recorded.
WARN	Log messages that indicate a noncritical service error and all higher-severity log messages are recorded.
INFO	Log messages that indicate service life-cycle events and provide other related crucial information, and all higher-severity log messages are recorded.
DEBUG	Log messages that convey extra information regarding life-cycle events and all higher-severity log messages are recorded.
TRACE	Log messages that are directly associated with any activity that corresponds to requests and all higher-severity log messages are recorded.
ALL	Log messages of all severity levels are recorded.

Release History Table

Release	Description
16.1R1	From Junos Space Network Management Platform Release 16.1R1 onward, you can configure log levels for JBoss and OpenNMS logs in Junos Space from the Administration workspace in the Junos Space Platform UI.

RELATED DOCUMENTATION

System Status Log File Overview | **1408**

Generating JBoss Thread Dump for Junos Space Nodes

From the Junos Space Network Management Platform UI, you can generate JBoss thread dumps for Junos Space nodes that are part of the Junos Space fabric. The thread dump can be generated for nodes that have the JBoss server running and are in the UP state, and also have the App Logic in the UP state.

NOTE: You cannot generate the JBoss thread dump for dedicated database nodes and dedicated Cassandra nodes.

The generated JBoss thread dump helps you troubleshoot problems with the JBoss server on that particular node.

You can generate JBoss thread dumps for one or more JBoss nodes from the Fabric page of the Administration workspace. You must be assigned the System Administrator role to be able to generate the JBoss thread dump for a node.

To generate the JBoss thread dump:

1. On the Junos Space Platform UI, select **Administration** > **Fabric**.

   The Fabric page appears, displaying all the nodes in the Junos Space fabric.

2. Right-click the JBoss node or nodes for which you want to generate the JBoss thread dump and select **Generate Thread Dump**. Alternatively, select the check boxes next to the node names and select **Generate Thread Dump** from the Actions menu.

   The JBoss Thread Dump dialog box appears.

3. Perform one of the following actions on the basis of whether you want to save the JBoss thread dump on the Junos Space node or on a remote server.

   - Select **Local** in the Mode field to save the JBoss thread dump on the Junos Space node.

     The JBoss thread dump is stored in the **/var/cache/jboss/thread_dumps/** directory on the Junos Space node.

   - Select **Remote** in the Mode field to save the JBoss thread dump on a remote server.

     All the remaining fields in the JBoss Thread Dump dialog box are enabled.

     To specify the remote server where you want the JBoss thread dump to be saved:

     a. In the **IP Address** field, enter the IP address of the remote server.

        The IP address can be either an IPv4 address or an IPv6 address.

     b. In the **Port** field, enter the port number.

        The default port number is 22.

     c. In the **Directory** field, enter the directory on the remote server where you want to save the JBoss thread dump.

> **NOTE:** Before you specify a directory in the **Directory** field, you must ensure that it exists on the remote server. If the specified directory does not exist on the remote server, the job fails, displaying a message that the directory is invalid.

d. In the **User Name** field, enter the username.

e. In the **Password** field, enter the password.

f. In the **Confirm Password** field, reenter the password.

g. (Optional) In the **Fingerprint** field, enter the fingerprint of the remote server.

4. Click **Generate** to generate the JBoss thread dump.

   The Generate Thread Dump Information dialog box appears, displaying the job ID link. Click the job ID to view the job on the Job Management page.

If you saved the JBoss thread dump to the Junos Space node, you can download it to your computer from the View Job Details page that appears when you double-click the job on the Job Management page.

The thread dump is saved as a compressed zip file with the filename format **threadDump_*timestamp***, where *timestamp* represents the date and time when the thread dump is generated.

An audit log entry is added when you generate the JBoss thread dump for a Junos Space node.

Release History Table

Release	Description
16.1R1	From the Junos Space Network Management Platform UI, you can generate JBoss thread dumps for Junos Space nodes that are part of the Junos Space fabric.

RELATED DOCUMENTATION

Downloading the Troubleshooting Log File in Server Mode | 1417

Downloading the Troubleshooting Log File in Maintenance Mode | 1420

Downloading Troubleshooting System Log Files Through the Junos Space CLI | 1421

Downloading the Troubleshooting Log File in Server Mode

You download the troubleshooting log file in Server mode when you want to view the contents of the troubleshooting log file and fix issues. You need to have the privileges of a System Administrator to download the troubleshooting log file.

Before you download the troubleshooting log file in Server mode:

- Ensure that you check the available disk space on the Junos Space node. The **Lack Of Space** error message is displayed if the disk space is insufficient.
- Ensure that a troubleshooting log download job you triggered earlier is not in progress. An error message is displayed if you trigger another troubleshooting log download job while a previous download job is in progress.

> **NOTE:** On a multinode setup, the troubleshooting log file is stored at the following location on the Junos Space node that completes the job: **/var/cache/jboss/space-logs**. You cannot download the troubleshooting log file if this node goes down.

To download the troubleshooting log file in Server mode:

1. On the Junos Space Network Management Platform user interface, select **Administration > Space Troubleshooting**.

   The Space Troubleshooting page is displayed.

2. Select whether to download the troubleshooting log file now or later.

   - To download the troubleshooting log file now:

     i. Click **Download**.

     The Collect Junos Space Logs Job Information dialog box is displayed.

     ii. Click **OK** in the dialog box.

     You can download the troubleshooting log file from the Job Management page.

     iii. Double-click the ID of the troubleshooting log collection job on the Job Management page.

     The Job Details dialog box is displayed.

     iv. Click the **Download** link to access the **troubleshoot_*yyyy-mm-dd_hh-mm-ss*.zip** file in your browser.

     The filename of the troubleshoot zip file includes the server Coordinated Universal Time (UTC) date and time. For example, **troubleshoot_2010-04-01_11-25-12.zip**.

     - If you are using Mozilla Firefox: In the Opening troubleshoot zip dialog box, click **Save file**, then click **OK** to save the zip file to your computer using the Firefox Downloads dialog box.
     - If you are using Internet Explorer: From the File Download page, click **Save** and select a directory on your computer where you want to save the **troubleshoot_*yyyy-mm-dd_hh-mm-ss*.zip** file.

     > **NOTE:** If the download job failed, the Job Details dialog box displays the reason the job failed.

     Table 183 lists the files included in the **troubleshoot_*yyyy-mm-dd_hh-mm-ss*.zip** file.

     Table 183: Log Files in the Troubleshooting Log File and Their Location

Log File Description	Location
System status log file	/var/log/SystemStatusLog
JBoss log files	**/var/log/jboss/***
Service provisioning data files	**/var/tmp/jboss/debug/***
MySQL error log file	**/var/log/mysqld.log**
Apache Web Server, NMA, and Web proxy log files	**/var/log/httpd/***

Table 183: Log Files in the Troubleshooting Log File and Their Location *(continued)*

Watchdog log files	**/var/log/watchdog/***
Linux system log messages	**/var/log/messages/***
CPU, RAM, or disk statistics (for the past 24 hours)	–
Heap and CPU Profiling Agent (HPROF) files	**/var/log/jboss**

- To download the troubleshooting log file later:

  i. Select the **Schedule at a later time** option button.

  ii. Enter the date in the **Date** field in the DD/MM/YYYY format.

  iii. Enter the time in the **Time** field in the hh:mm format.

  iv. Click **Download**.

  The troubleshooting log download job is triggered at the scheduled time. You can view the status of the scheduled job on the Job Management page.

  TIP: When you contact Juniper Technical Assistance Center, describe the problem you encountered and provide the **troubleshoot_*yyyy-mm-dd_hh-mm-ss*.zip** file to the JTAC representative.

3. Click **Close** to return to the Administration statistics page.

RELATED DOCUMENTATION

System Status Log File Overview | **1408**

Customizing Node System Status Log Checking | **1410**

Customizing Node Log Files to Download | **1412**

Downloading the Troubleshooting Log File in Maintenance Mode | **1420**

Downloading Troubleshooting System Log Files Through the Junos Space CLI | **1421**

Downloading the Troubleshooting Log File in Maintenance Mode

Maintenance Mode is a special mode that an administrator can use to perform system recovery or debugging tasks while all nodes in the fabric are shut down and the Web proxy is running.

The administrator can download the **troubleshoot_*yyyy-mm-dd_hh-mm-ss*.zip** file from Maintenance Mode. The troubleshoot zip file includes the server Coordinated Universal Time (UTC) date and time. For example, **troubleshoot_2010-04-01_11-25-12.zip**.

To download the troubleshooting log file in maintenance mode, perform the following steps:

1. Connect to a Junos Space Appliance in maintenance mode by using the Junos Space Appliance URL.

   For example:

   `https://<ipaddress>/maintenance`

   Where *ipaddress* is the address of the Junos Space Appliance.

   The Maintenance Mode page appears.

2. Click the **click here to log in** link. The login dialog box appears.

3. Log in to maintenance mode by using the authorized login name and password.

4. Click OK. The Maintenance Mode Actions menu appears.

5. Click **Download Troubleshooting Data and Logs**. The file download dialog box appears.

6. Click Save to download the **troubleshoot_*yyyy-mm-dd_hh-mm-ss*.zip** file to the connected computer.

7. Click **Log Out and Exit from Maintenance Mode**.

RELATED DOCUMENTATION

- Maintenance Mode Overview | **1153**
- System Status Log File Overview | **1408**
- Customizing Node System Status Log Checking | **1410**
- Customizing Node Log Files to Download | **1412**
- Downloading the Troubleshooting Log File in Server Mode | **1417**
- Downloading Troubleshooting System Log Files Through the Junos Space CLI | **1421**

Downloading Troubleshooting System Log Files Through the Junos Space CLI

IN THIS SECTION

- Downloading a System Log File by Using a USB Device | **1421**
- Downloading System Log File by Using SCP | **1423**

If a Junos Space node is Up, the administrator can log in to the Junos Space node and download system status logs for each fabric node by using the Secure Copy Protocol (SCP). If the Junos Space node is Down but you can log in to the console of a Junos Space Appliance, you can download system status logs to a USB drive.

The **Retrieve Logs** utility collects all system log files in the **/var/log** subdirectory and creates a compressed TAR file (extension ***.tgz**). For more information about the log files that are written, see "System Status Log File Overview" on page 1408.

This topic includes the following sections:

Downloading a System Log File by Using a USB Device

Using the **Retrieve Logs** > **Save to USB Device** command, the administrator can download system status logs to a connected USB device if the Junos Space node is Down and you can log in to the console.

Before you begin, ensure that the USB device is connected to the Junos Space Appliance.

1. Log in to the Junos Space Appliance using the administrator username (admin) and password.

   The Junos Space Settings Menu appears, as shown.

```
Junos Space Settings Menu

1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> (Debug) run shell

Q> Quit
R> Redraw Menu

Choice [1-6,QR]:
```

2. Type **4** at the prompt.

   The Retrieve Logs submenu appears.

```
Choice [1-6,AQR]: 4
1> Save to USB Device
2> Send Using SCP

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-2,AMR]:
```

3. Type **1**.

   The following message is displayed: **This process will retrieve the log files on all cluster members and combine them into a .tar file. Once the file is created, you can copy the files onto a USB drive. Continue? [y/n]**

4. Type **y** to continue.

   You are prompted to enter the administrator password.

5. Enter the administrator password.

The system downloads the log files from all the nodes in the fabric and combines them into a **.tar** file. After the file is created, the file is coped to the USB device and a message similar to the following is displayed: **Copying 20090827-1511-logs.tar to USB drive**.

> **NOTE:** If the USB device is not ready, the following message appears: **Log collection complete If USB key is ready, press "Y". To abort, press "N".**

6. After the files are copied, unmount the USB and eject it from the Junos Space Appliance.

Downloading System Log File by Using SCP

Using the Junos Space CLI **Retrieve Logs** > **SCP** command, the administrator can download system status logs to a specific location.

To download system status logs by using SCP, perform the following steps:

1. Log in to the Junos Space node using the administrator username (admin) and password.

   The Junos Space Settings Menu appears, as shown.

```
Junos Space Settings Menu

1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> (Debug) run shell

Q> Quit
R> Redraw Menu

Choice [1-6,QR]:
```

2. Type **4** at the prompt.

   The Retrieve Logs submenu appears.

```
Choice [1-6,AQR]: 4
1> Save to USB Device
2> Send Using SCP
```

```
A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-2,AMR]:
```

3. Type **2**.

   The following confirmation message is displayed:

   This process will retrieve the log files on all cluster members and combine them into a .tar file. Once the file is created, you will be asked for a remote scp server to transfer the file to. Continue? [y/n]

4. Type **y** to continue.

   You are prompted to enter the administrator password.

5. Enter the administrator password.

   A message indicating that the log files are being collected is displayed. The process retrieves the log files on all cluster members and combines them into a **.TAR** file. This might take a few minutes to complete.

   After this is completed, you are prompted to enter the IP address of the remote server.

6. Enter the IP address of the SCP server to which to transfer the file.

   NOTE:
   - Depending on whether the Junos Space fabric is configured with only IPv4 addresses or both IPv4 and IPv6 addresses, Junos Space Platform allows you to enter an IPv4 address or either an IPv4 or IPv6 address respectively for the SCP server.
   - The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to http://www.iana.org/assignments/ipv4-address-space for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space for the list of restricted IPv6 addresses.

7. Enter the remote SCP user.

8. Enter the directory on the remote SCP server where the log file should be stored; for example, **/root/tmplogs**.

   The remote server information that you entered is displayed. The following is a sample:

```
Remote scp IP: 192.0.2.0
Remote scp user: root
Remote scp path: /root/tmplogs
Is this correct? [y/n]
```

9. If the SCP server information is correct, type **y**.

   If you are connecting to the SCP server for the first time, a message is displayed asking you to confirm that you want to continue. The following is a sample message:

```
The authenticity of host '192.0.2.0 (192.0.2.0)' can't be established.
RSA key fingerprint is 01:70:4c:47:9e:1e:84:fc:69:3c:65:99:6d:e6:88:87.
Are you sure you want to continue connecting (yes/no)? yes
```

> **NOTE:** If the SCP server information is incorrect or if you want to modify the SCP server information, type **n** at the prompt, and modify the SCP server information as explained in the preceding steps.

10. Type **y** to continue.

    You are prompted to enter the password.

11. Enter the password for the SCP server.

    If the credentials are correct, the file is transferred to the SCP server.

RELATED DOCUMENTATION

- Maintenance Mode Overview | **1153**
- System Status Log File Overview | **1408**
- Customizing Node System Status Log Checking | **1410**
- Customizing Node Log Files to Download | **1412**
- Downloading the Troubleshooting Log File in Server Mode | **1417**
- Downloading the Troubleshooting Log File in Maintenance Mode | **1420**

CHAPTER 74

Managing Certificates

IN THIS CHAPTER

- Certificate Management Overview | 1426
- Changing User Authentication Modes | 1434
- Installing a Custom SSL Certificate on the Junos Space Server | 1441
- Uploading a User Certificate | 1445
- Uploading a CA Certificate and Certificate Revocation List | 1448
- Deleting a CA Certificate or Certificate Revocation List | 1450
- Adding and Activating X.509 Certificate Parameters for X.509 Certificate Parameter Authentication | 1451
- Modifying an X.509 Certificate Parameter | 1454
- Deleting X.509 Certificate Parameters | 1455

Certificate Management Overview

IN THIS SECTION

- Authentication Modes Workflow | 1427
- Custom Junos Space Server Certificates | 1429
- Certificate Attributes | 1429
- User Certificates | 1431
- CA Certificates and CRLs | 1432
- Changing the User Authentication Mode | 1432
- Certificate Expiry | 1432
- Invalid User Certificates | 1433

Typically, users gain access to resources from an application or system on the basis of their username and password. You can also use certificates to authenticate and authorize sessions among various servers and users. Certificate-based authentication over a Secure Sockets Layer (SSL) connection is the most secure type of authentication. The certificates can be stored on a smart card, a USB token, or a computer's hard drive. Users typically swipe their smart card to log in to the system without entering their username and password.

Junos Space Network Management Platform is shipped with the default password-based authentication mode. Administrators can use the default credentials to log in to Junos Space Platform. Junos Space Platform allows you to use certificate-based authentication and from Junos Space Network Management Platform Release 15.2R1 onward, X.509 parameter-based authentication as well, to authenticate users. These authentication modes can be configured from the User section on the Modify Application Settings page in the Administration workspace.

By default, Junos Space Platform uses a self-signed SSL certificate. However, if you need to use your own custom certificate, you can upload your custom certificate in the X.509 or PKCS#12 format. With the complete certificate validation mode, the entire X.509 certificate is validated during the login process and you must upload user certificates for all users.

During X.509 parameter-based authentication, you can specify up to four X.509 certificate parameters per user that are validated during the login process. With the X.509 parameter-based authentication, you can avoid uploading certificates for new users to Junos Space Platform. Junos Space Platform extracts the values of the parameters for existing users from the certificates loaded when the users were created. You can define the X.509 certificate parameters in the X509-Certificate-Parameters section on the Modify Application Settings page in the Administration workspace.

> **NOTE:** Only one authentication mode is supported at a time and all users are authenticated using the selected authentication mode.

See the following sections for information about workflow for authentication modes, custom Junos Space server certificates, user certificates, certificate authority (CA) certificates, certificate revocation lists (CRL), and certificate expiry and invalidity conditions on Junos Space Platform.

Authentication Modes Workflow

The steps in establishing an SSL connection for the different modes of authentication are as follows:

- Username and password–based authentication:
  1. A client requests access to the Junos Space server.
  2. The Junos Space server presents its certificate to the client.
  3. The client verifies the server's certificate.

4. If the verification of the certificate is successful, then the client sends its username and password to the server.
5. The server verifies the credentials of the client.
6. If the verification is successful, then the server grants access to the protected resource requested by the client.

- Certificate-based authentication:
  1. A client requests access to the Junos Space server.
  2. The Junos Space server presents its certificate to the client.
  3. The client verifies the server's certificate.
  4. If the verification of the certificate is successful, then the client sends its certificate to the server.
  5. The server verifies the client's certificate.
  6. If the verification is successful, then the server grants access to the protected resource requested by the client.

     If the verification is unsuccessful, Junos Space Platform displays a login failure page to the user.
- X509 certificate parameter–based authentication:
  1. A client requests access to the Junos Space server.
  2. The Junos Space server presents its X.509 certificate to the client.
  3. The client verifies the server's X.509 certificate.
  4. If the verification of the certificate is successful, then the client sends its certificate to the server.
  5. The server extracts the specified values from the client's X.509 certificate and validates the values with those in the Junos Space Platform database.
  6. If the verification is successful, then the server grants access to the protected resource requested by the client.

     If the verification is unsuccessful, Junos Space Platform displays a login failure page to the user.

> **NOTE:** When using complete certificate-based or certificate parameter–based authentication, the session is terminated if the smart or secure card (containing the certificate and the private key) that is used for logging in is unplugged or removed from the client system.

Custom Junos Space Server Certificates

By default, Junos Space Network Management Platform uses a self-signed SSL certificate. However, if you need to use your own custom certificate, go to **Administration > Platform Certificate** page and upload your custom X.509 or PKCS#12 certificate on the Platform Certificate page.

X.509 is a widely used standard for defining digital certificates. Typically, in X.509, the certificate and the key are stored separately. The private key can be either encrypted or unencrypted. Although a passphrase is optional, it is required if the private key is encrypted.

The Personal Information Exchange Syntax Standard (PKCS) #12 format is a widely used format for digital certificates in the Windows operating system. This standard specifies a portable format for storing or transporting a user's private keys, certificates, and passphrases in one encryptable file.

For instructions to upload your custom certificate, see "Installing a Custom SSL Certificate on the Junos Space Server" on page 1441.

Certificate Attributes

Table 184 lists the attributes that you commonly see in a certificate.

Table 184: Certificate Attributes

Certificate Attribute	Description
Subject Name: OID.1.2.840.113549.1.9.1=user1@10.205.57.195	"OID.1.2.840.113549.1.9.1" is the ASN.1 object identifier used to identify this signature algorithm. "user1@10.205.57.195" is the e-mail address of the certificate owner.
Subject Name: CN	Common name of the certificate owner
Subject Name: OU	Name of the organizational unit to which the certificate owner belongs For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains "**Junos Space**" for this attribute.
Subject Name: O	Organization to which the certificate owner belongs For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains "**Juniper Networks, Inc.**" for this attribute.

Table 184: Certificate Attributes *(continued)*

Certificate Attribute	Description
Subject Name: L	Certificate owner's location For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains "**Sunnyvale**" for this attribute.
Subject Name: ST	Certificate owner's state of residence For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains "**California**" for this attribute.
Subject Name: C	Certificate owner's country of residence For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains "**US**" for this attribute.
Issuer Name: OID.1.2.840.113549.1.9.1=user1@10.205.57.195	"OID.1.2.840.113549.1.9.1" is the ASN.1 object identifier used to identify this signature algorithm. "user1@10.205.57.195" is the e-mail address of issuer.
Issuer Name: CN	Common name of the certificate issuer It is the IP address of the system. The common name (CN) must match the hostname of the issuer of this certificate. In general, it should be the hostname of issuer.
Issuer Name: OU	Name of the organizational unit to which the certificate issuer belongs For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains "**Junos Space**" for this attribute.
Issuer Name: O	Organization to which the certificate issuer belongs For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains "**Juniper Networks, Inc.**" for this attribute.

Table 184: Certificate Attributes *(continued)*

Certificate Attribute	Description
Issuer Name: L	Certificate issuer's location For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains "**Sunnyvale**" for this attribute.
Issuer Name: ST	Certificate issuer's state of residence For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains "**California**" for this attribute.
Issuer Name: C	Certificate issuer's country of residence For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks contains "**US**" for this attribute.
Signature Algorithm Name	Algorithm used by the Certificate Authority to sign the certificate For example, the Junos Space Network Management Platform SSL certificate signed by Juniper Networks can contain "**SHA1withRSA**" for this attribute.
Serial Number	Certificate's serial number
Not Before	Date at which the certificate becomes valid
Not After	Date at which the certificate becomes invalid

User Certificates

If you use certificate-based authentication mode, then for each user you need to upload the corresponding certificate for the Junos Space server to authenticate the user. You can associate a certificate with a user when you create the user or by modifying the user settings. To associate a certificate with an existing user, go to **Role Based Access Control > User Accounts > Select a user > Modify User** page.

For instructions to upload a user certificate, refer to "Uploading a User Certificate" on page 1445.

CA Certificates and CRLs

A certification authority (CA) certificate or the root certificate is used to verify a user certificate. The private key of the root certificate is used to sign the user certificates, which then inherit the trustworthiness of the root certificate.

A certificate revocation list (CRL), which is maintained by a CA, is a list of certificates that were issued and revoked by that CA before their scheduled expiration date, along with the reasons for revocation. A CA may revoke a certificate for various reasons, such as the user specified in the certificate may no longer have the authority to use the key, the key specified in the certificate might have been compromised, another certificate is replacing the current certificate, and so on.

For instructions to upload CA certificates or CRLs, refer to "Uploading a CA Certificate and Certificate Revocation List" on page 1448.

Changing the User Authentication Mode

You can change the authentication mode from username and password-based to certificate-based or X.509 certificate parameter–based from the Junos Space user interface or from the CLI of the VIP node. You must upload the certification authority (CA) certificates and the personal or user certificates (the Junos Space server certificate is optional) to the Junos Space server before changing the authentication mode. Junos Space Platform verifies all certificates before they are uploaded. Invalid or badly formed certificates are not uploaded.

CAUTION: When the authentication mode is changed, all existing user sessions, except that of the current administrator who is changing the authentication mode, are automatically terminated and the users are forced to log out. You need not restart Junos Space Platform when you switch from one authentication mode to another.

For instructions to change authentication modes, refer to "Changing User Authentication Modes" on page 1434.

Certificate Expiry

When the X.509 Junos Space server certificate is scheduled to expire within 30 days from the current date, Junos Space Platform displays a warning message every time the administrator logs in. For example: **Your platform certificate is going to expire on May 24, 2015. Space will automatically use default certificate if your certificate will expire within 1 day. Change platform certificate using "Administration > Platform Certificate" page. Would you like to change it now?**

As an administrator, perform one of the following actions:

- Upload a new certificate—Select **Administration > Platform Certificate** and upload the certificate from the Upload Certificate area. Junos Space Platform deletes the old user certificate and starts using the newly uploaded certificate.
- Use the default certificate—Select **Administration > Platform Certificate** and click **Use Default Certificate** in the Current Platform Certificate area.

> **NOTE:** When the X.509 Junos Space server certificate is scheduled to expire in a day, Junos Space Platform starts using the default self-signed certificate. The self-signed Junos Space Platform SSL certificate created during installation has a five-year validity.

When a user certificate is scheduled to expire within 30 days from the current date, Junos Space Platform displays a warning message if the user has logged in using the certification-based authentication mode. For more information, refer to "Uploading a User Certificate" on page 1445.

Invalid User Certificates

A user certificate could become invalid for the following reasons:

- Certificate is expired.
- Certificate expires within a day.
- Certificate will be valid only later.
- Certificate does not match the private key.
- Certificate or private key file is broken.
- Same certificate exists in the Junos Space server.

If a user tries to log in with an invalid or expired certificate, Junos Space Platform displays a login failure page with the following error message: **No user mapped for this certificate**.

Release History Table

Release	Description
15.2R1	Junos Space Platform allows you to use certificate-based authentication and from Junos Space Network Management Platform Release 15.2R1 onward, X.509 parameter-based authentication as well, to authenticate users.

RELATED DOCUMENTATION

Installing a Custom SSL Certificate on the Junos Space Server | 1441
Uploading a CA Certificate and Certificate Revocation List | 1448

Changing User Authentication Modes

IN THIS SECTION

- Changing the User Authentication Mode from Password-Based to Complete Certificate-Based from the User Interface | 1435
- Changing the User Authentication Mode from Complete Certificate-Based to Certificate Parameter–Based from the User Interface | 1437
- Changing the User Authentication Mode from Certificate Parameter–Based to Complete Certificate-Based from the User Interface | 1439
- Changing the User Authentication Mode to Password-Based from the User Interface | 1440
- Changing the User Authentication Mode to Password-Based from the CLI | 1440

You change the authentication mode to authenticate users by using credentials (username and password), certificates, or X.509 certificate parameters.

CAUTION: When you change the authentication mode from the user interface or the CLI, all existing user sessions, except that of the current administrator who is changing the authentication mode, are automatically terminated and the users are forced to log out. You need not restart Junos Space Platform when you switch from one authentication mode to another.

NOTE: An audit log entry is generated when you change the authentication mode.

The following topics describe the steps to change user authentication modes.

Changing the User Authentication Mode from Password-Based to Complete Certificate-Based from the User Interface

You change the authentication mode from password-based to complete certificate–based when the users must be authenticated on the basis of their certificates.

To change the user authentication mode from password-based to complete certificate–based:

1. (Optional) Load the server certificate to the Junos Space server:

   a. Go to **Administration > Platform Certificate**.

      The Platform Certificate page appears.

   b. Upload the certificate from the Upload Certificate area.

   If you do not upload a customized server certificate, then the default Junos Space Network Management Platform certificate is used.

   For more information about loading the server certificate, refer to "Installing a Custom SSL Certificate on the Junos Space Server" on page 1441.

2. Load the user certificate:

   - For a new local user, load the user certificate from the **Role Based Access Control > User Accounts > Create User** page.
   - For existing local users, load the user certificate from the **Role Based Access Control > User Accounts > Modify User** page or by clicking the **User Settings** icon on the Junos Space banner.

   For more information about loading user certificates, refer to "Uploading a User Certificate" on page 1445.

3. Load the CA certificates and the certificate revocation list to the Junos Space server:

   a. Go to **Administration > CA/CRL Certificates**.

      The CA/CRL Certificates page appears.

   b. Upload the CA certificates and the certificate revocation list on the CA/CRL Certificates page.

   For more information about loading CAs and CRLs, refer to "Uploading a CA Certificate and Certificate Revocation List" on page 1448.

4. Enable certificate–based authentication mode:

   a. Navigate to **Administration > Applications > Network Management Platform > Modify Application Settings** page.

   b. Click the **User** link (on the left of the page).

   c. Select the **Use X509 Certificate Complete Certificate** option button.

   d. Click **Modify**.

      A confirmation dialog box is displayed.

   e. You can change the authentication mode to certificate–based or retain the password-based mode.

      - To change the authentication mode, click **Yes**.

        Jobs are triggered to change the login password and FMPM password and switch the authentication mode to complete certificate–based. You can view the details of the jobs on the Job Management page.

        An error message is displayed if you have not loaded the required certificates.

      - To retain the authentication mode, click **No**.

The authentication mode is changed to complete certificate–based authentication.

Changing the User Authentication Mode from Complete Certificate-Based to Certificate Parameter–Based from the User Interface

You change the authentication mode from complete certificate–based to certificate parameter–based when the users must be authenticated by using certificate parameters.

To change the user authentication mode from complete certificate–based to certificate parameter–based:

1. Specify the parameters to be validated:

   a. Go to **Administration > Applications > Network Management Platform > Modify Application Settings**.

      The Modify Application Settings page appears.

   b. Click the **X509CertificateParameters** link.

      The X509CertificateParameters page appears.

   c. Add the parameters to be validated.

   For more information about adding X.509 certificate parameters, refer to "Adding and Activating X.509 Certificate Parameters for X.509 Certificate Parameter Authentication" on page 1451.

2. Specify the values for the parameters:

   - For a new local user, enter the values from the **Role Based Access Control > User Accounts > Create User** page.
   - For existing local users, Junos Space Platform extracts the values for the specified parameters when you change the authentication mode.

3. Enable certificate parameter–based authentication mode:

   a. Navigate to **Administration > Applications > Network Management Platform > Modify Application Settings**.

   b. Click the **User** link (on the left of the page).

   c. Select the **Use X509 Certificate Parameters** option button.

   d. Click **Modify**.

      A confirmation dialog box is displayed.

   e. You can change the authentication mode to certificate parameter–based or retain the certificate–based mode.

      - To change the authentication mode, click **Yes**.

        Jobs are triggered to parse the parameters of user certificates, change the login password and FMPM password and switch the authentication mode to certificate parameter–based. You can view the details of the jobs on the Job Management page.

        An error message is displayed if you have not added and activated the parameters.

      - To retain the authentication mode, click **No**.

The authentication mode is changed to certificate parameter–based authentication.

Changing the User Authentication Mode from Certificate Parameter–Based to Complete Certificate-Based from the User Interface

You change the authentication mode from certificate parameter–based to complete certificate–based when the users must be authenticated on the basis of their certificates.

> **NOTE:** You must upload certificates for all new users (added after previously changing the authentication mode to certificate parameter–based) before changing the authentication mode from certificate parameter–based to complete certificate–based.

To change the user authentication mode from certificate parameter–based to complete certificate–based:

1. Enable complete certificate-based authentication mode:
   a. Navigate to **Administration > Applications > Network Management Platform > Modify Application Settings**.
   b. Click the **User** link (on the left of the page).
   c. Select the **Use X509 Certificate Complete Certificate** option button.
   d. Click **Modify**.

      A confirmation dialog box is displayed.
   e. You can change the authentication mode to certificate–based or retain the certificate parameter–based mode.
      - To change the authentication mode, click **Yes**.

        Jobs are triggered to change the login password and FMPM password and switch the authentication mode to complete certificate–based. You can view the details of the jobs on the Job Management page.

        An error message is displayed if you have not loaded the certificates for new users.
      - To retain the authentication mode, click **No**.

The authentication mode is changed to complete certificate–based authentication.

Changing the User Authentication Mode to Password-Based from the User Interface

You change the authentication mode to password-based when the users must be authenticated by using passwords.

To change the user authentication mode to password-based authentication from the user interface:

1. Navigate to **Administration > Applications > Network Management Platform > Modify Application Settings**.
2. Click the **User** link (on the left of the page).
3. Select the **Use User Password Auth Mode** option button.
4. Click **Modify**.

   A confirmation dialog box is displayed.
5. You can change the authentication mode to password-based or retain the current authentication mode.
   - To change the authentication mode, click **Yes**.

     Jobs are triggered to send the passwords to users by their e-mail addresses in Junos Space Platform and switch the authentication mode to password-based. You can view the details of the jobs on the Job Management page.
   - To retain the authentication mode, click **No**.

The authentication mode is changed to password-based authentication.

Changing the User Authentication Mode to Password-Based from the CLI

You change the authentication mode to password-based from the CLI when users are restricted from logging in by using certificate–based authentication mode.

To change the authentication mode to password-based authentication from the CLI:

1. Log in to the CLI of the Junos Space server running as the VIP node, as the root user.
2. Navigate to the following directory: **/var/www/cgi-bin**.
3. Type the following command from the **./setSpaceAuthMode password-based** directory:

   The authentication mode is changed to password-based and users can login with their username and password.

RELATED DOCUMENTATION

Certificate Management Overview | 1426

Installing a Custom SSL Certificate on the Junos Space Server | 1441

Adding and Activating X.509 Certificate Parameters for X.509 Certificate Parameter Authentication | 1451

Installing a Custom SSL Certificate on the Junos Space Server

IN THIS SECTION

- Installing an X.509 Junos Space Server Certificate | 1441
- Installing a Junos Space Server Certificate in the PKCS #12 Format | 1443
- Reverting to the Default Junos Space Server SSL Certificate | 1444

By default, Junos Space Network Management Platform uses a self-signed SSL certificate. However, Junos Space Network Management Platform provides an option to associate your own custom SSL certificate with the Junos Space server.

You install a custom SSL certificate to use X.509 certificate–based authentication mode. You can upload a certificate in X.509, PKCS#1, or PKCS # 12 format. If you upload the certificate in the PKCS#1 or PKCS#12 format, Junos Space Network Management Platform converts the certificate into two files (public certificate and decrypted private key) in the Privacy-Enhanced Mail (PEM) format.

CAUTION: When the authentication mode is changed, all existing user sessions, except that of the current administrator who is changing the authentication mode, are automatically terminated and the users are forced to log out.

The topics in this section describe how to associate your own custom SSL certificate with the Junos Space server.

Installing an X.509 Junos Space Server Certificate

You install an X.509 certificate file on the Junos Space server to enable X.509 certificate–based authentication. Before you upload and install the certificate, ensure that both the certificate and the key are available on your local computer.

To install an X.509 certificate file:

1. Select **Network Management Platform > Administration > Platform Certificate**.

   The Platform Certificate page appears.

2. From the Upload Certificate area, select the **X.509 Certificate & Private Key** option button to upload the certificate files in the Distinguished Encoding Rules (DER) or Privacy-Enhanced Mail (PEM) format.

   By default, this option is selected.

   - DER format certificate files:
     - The supported extensions are: **.der**, **.cer**, and **.crt**.
     - They are stored in binary format.
   - PEM format certificate files:
     - The supported extensions are: **.pem**, **.cer**, and **.crt**.
     - They are stored in the Base64-encoded DER format.

3. To navigate to select the X.509 certificate file from your local file system, click **Browse** adjacent to the **Certificate** field.

4. To navigate to and select the private key file from your local file system, click **Browse** adjacent to the **Private Key** field.

5. (Optional) Enter the passphrase in the **Private Key Pass-phrase** field.

   You must enter the passphrase if the private key is encrypted.

6. Click **Upload**.

Junos Space Platform displays a warning message asking for confirmation to replace the current certificate.

7. You can either install the certificate or cancel the installation process.

   - To install the certificate, click **Yes**.

     Junos Space Platform performs internal validations to verify whether the uploaded files are valid. If any of the files is invalid, Junos Space Platform displays an error message.

     If the files are valid, then the upload is successful and Junos Space Platform starts using the new certificate. All existing sessions are terminated and the users are forced to log out.

   - To cancel the installation, click **Cancel**.

     Junos Space Platform continues to use the current certificate.

Installing a Junos Space Server Certificate in the PKCS #12 Format

Before you proceed, make sure that the PKCS #12 certificate is available on your local file system.

To upload a certificate in PKCS#12 format:

1. Select **Network Management Platform > Administration > Platform Certificate**.

   The Platform Certificate page appears.

2. From the Upload Certificate area, select the **PKCS #12 Format Certificate** option button to upload the PKCS#12 format certificate file.

3. To navigate to and select the PKCS#12 format certificate file from your local file system, click **Browse** adjacent to the **Certificate & Private Key** field.

4. (Optional) Enter the password in the **Password** field.

5. Click **Upload**.

Junos Space Platform displays a warning message asking for confirmation to replace the current certificate.

6. You can either install the certificate or cancel the installation process.

   - To install the certificate, click **Yes**.

     Junos Space Platform performs internal validations to verify whether the uploaded files are valid. If any of the files is invalid, Junos Space Platform displays an error message.

     If the files are valid, then the upload is successful and Junos Space Platform starts using the new certificate. All existing sessions are terminated and the users are forced to log out.

   - To cancel the installation, click **Cancel**.

     Junos Space Platform continues to use the current certificate.

Reverting to the Default Junos Space Server SSL Certificate

You revert to the default certificate when your current certificate is about to expire.

To revert to the default certificate:

1. Select **Network Management Platform > Administration > Platform Certificate**.

   The Platform Certificate page appears.

   The Current Platform Certificate area of the page displays the certificate that is currently being used by the Junos Space server. To gain an understanding about the attributes of the certificate, see "Certificate Management Overview" on page 1426.

2. To revert to the default SSL certificate, click **Use Default Certificate**.

   An information dialog box indicating that the default self-signed Juniper Networks certificate will be used is displayed.

3. You can continue or cancel reverting to the default certificate.

   - To use the default certificate, click **OK**.

     Junos Space Platform uses the default certificate.

   - To cancel, click **Cancel**.

     Junos Space Platform uses the custom certificate.

RELATED DOCUMENTATION

Certificate Management Overview | **1426**

Uploading a User Certificate | **1445**

Uploading a CA Certificate and Certificate Revocation List | **1448**

Changing User Authentication Modes | **1434**

Uploading a User Certificate

IN THIS SECTION

- Uploading a User Certificate for a New User | **1445**
- Uploading a User Certificate for an Existing User | **1446**
- Uploading Your User Certificate | **1447**

You upload user certificates if you enabled X.509 certificate–based authentication.

Before you proceed, make sure that the user certificate is available on your local system.

Uploading a User Certificate for a New User

You upload user certificates when the new user must be authenticated by using certificate-based authentication.

NOTE: You must be assigned the privileges of a user administrator to upload user certificates.

To upload a certificate for a new user:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > User Accounts** and click the **Create User** icon.

   The Create User page appears.

2. Enter values for the mandatory fields on the Create User page.

   For detailed information about the fields that appear on the Create User page, see "Creating Users in Junos Space Network Management Platform" on page 1035.

3. Click **Browse** adjacent to the **X509 Cert File** field to navigate to the location of the X.509 certificate file on your local system.

4. Select the X.509 certificate file and click **Upload**.

5. Click **Finish**.

   The user certificate for the new user is uploaded to Junos Space Platform.

Uploading a User Certificate for an Existing User

You upload a user certificate for an existing user before you enable certificate-based authentication or when you switch from parameter-based authentication to certificate based authentication (only for users who were added to Junos Space Platform after switching from certificate-based to parameter-based).

To upload a user certificate for an existing user:

1. On the Junos Space Network Management Platform user interface, select **Role Based Access Control > User Accounts**.

   The User Accounts page appears.

2. Select the user and click the **Modify User** icon.

   The Modify User page appears.

3. Click **Browse** adjacent to the X509 Cert File field to navigate to the location of the X.509 certificate file on your local system.

4. Select the X.509 certificate file and click **Upload**.

5. Click **Finish**.

   The user certificate for the existing user is uploaded to Junos Space Platform.

Uploading Your User Certificate

You upload your user certificate when you need to add your user certificate or renew the existing user certificate.

To upload your user certificate:

1. On the Junos Space Network Management Platform user interface, click the **User Settings** icon located at the top-right corner of the Junos Space Platform user interface (next to the Log Out icon).

   The Change User Settings pop-up window is displayed.

2. Click the **X.509 Certificate** tab.

3. In the Certificate Subject Name field, enter the string that needs to be secured.

   For example, it could be a person's e-mail address, a website address, or a system's IP address, and so on.

4. Click **Browse** adjacent to the X.509 Certificate File field to navigate to the location of the X.509 certificate file on your local system.

5. Select the X.509 certificate file and click **Upload**.

6. Click **OK**.

   Your certificate file is uploaded to Junos Space Platform.

RELATED DOCUMENTATION

Certificate Management Overview | 1426

Installing a Custom SSL Certificate on the Junos Space Server | 1441

Uploading a CA Certificate and Certificate Revocation List | 1448

Uploading a CA Certificate and Certificate Revocation List

IN THIS SECTION

- Uploading a CA Certificate | 1448
- Uploading a Certification Revocation List | 1449
- Deleting CA Certificates or Certificate Revocation Lists | 1449

You upload a certification authority (CA) certificate or the root certificate to verify user certificates. You upload a certificate revocation list (CRL) to maintain a list of certificates that were issued and revoked by that CA.

Uploading a CA Certificate

Before you proceed, make sure that the CA certificate is available on your local system.

To upload a CA certificate:

1. On the Junos Space Network Management Platform user interface, select **Administration > CA/CRL Certificates**.

   The CA/CRL Certificates page appears. This page displays the CA certificates that were previously uploaded to Junos Space Platform.

2. Click the down arrow next to the + icon and select **X.509 CA Certificate**.

   The Upload X.509 CA Certificate page appears.

3. • To upload the CA certificate:

   i. Click **Browse** adjacent to the X.509 CA Certificate File field to navigate to the location of the X.509 CA certificate file on your local system.

   ii. Click **Upload**.

   The CA certificate file is uploaded to Junos Space Platform.

   • To cancel the upload, click **Cancel**.

Uploading a Certification Revocation List

Before you proceed, make sure that the CRL is available on your local system.

To upload a CRL:

1. On the Junos Space Network Management Platform user interface, select **Administration > CA/CRL Certificates**.

   The CA/CRL Certificates page appears. This page displays the CRLs that were previously uploaded to Junos Space Platform.

2. Click the down arrow next to the + icon and select **X.509 CRL Certificate**.

   The Upload X.509 CRL Certificate dialog box appears.

3. • To upload the CRL:

   i. Click **Browse** adjacent to the X.509 CRL Certificate File field to navigate to the location of the X.509 CRL file on your local system.

   ii. Click **Upload**.

   The CRL is uploaded to Junos Space Platform.

   • To cancel the upload, click **Cancel**.

Deleting CA Certificates or Certificate Revocation Lists

To delete any CA certificates or CRLs:

1. On the Junos Space Network Management Platform user interface, select **Administration > CA/CRL Certificates**.

The CA/CRL Certificates page appears. This page displays the CRLs that were previously uploaded to Junos Space Platform.

2. Select the CA certificates or CRLs to delete and click the **Delete X509 CA/CRL Certificate** icon located at the top-left corner of the CA/CRL Certificates page.

   A confirmation dialog box is displayed.

3. Click **Yes** on the confirmation dialog box.

   The selected CAs or CRLs are deleted from Junos Space Platform.

RELATED DOCUMENTATION

Certificate Management Overview | **1426**

Installing a Custom SSL Certificate on the Junos Space Server | **1441**

Deleting a CA Certificate or Certificate Revocation List | **1450**

Deleting a CA Certificate or Certificate Revocation List

You delete a CA certificate when you do not want to trust a certificate authority in Junos Space Platform. You delete a CRL when you do not want to validate whether a certificate has been revoked.

To delete CA certificates or CRLs:

1. On the Junos Space Network Management Platform user interface, select **Administration > CA/CRL Certificates**.

   The CA/CRL Certificates page appears. This page displays the CRLs that were previously uploaded to Junos Space Platform.

2. Select the CA certificates or CRLs to delete and click the **Delete X509 CA/CRL Certificate** icon located at the top-left corner of the CA/CRL Certificates page.

   A confirmation dialog box is displayed.

3. Click **Yes** on the confirmation dialog box.

   The selected CAs or CRLs are deleted from Junos Space Platform.

RELATED DOCUMENTATION

Certificate Management Overview | 1426

Changing User Authentication Modes | 1434

Uploading a CA Certificate and Certificate Revocation List | 1448

Adding and Activating X.509 Certificate Parameters for X.509 Certificate Parameter Authentication

IN THIS SECTION

- Adding X.509 Certificate Parameters for X.509 Certificate Parameter Authentication | 1451
- Activating an X.509 Certificate Parameter | 1453

Starting with Junos Space Network Management Platform Release 15.2R1, you can add X.509 certificate parameters to authenticate users by using X.509 certificate parameters. You must enable X.509 certificate parameter authentication mode on the Modify Application Settings page to use this authentication mode. You can add up to four parameters to authenticate users in this authentication mode. You can specify X.509 certificate parameters such as CN (common name), OU (organizational unit), O (organization), L (location), ST (state of residence), C (country of residence), EMAILADDRESS (e-mail address), rfc822Name (e-mail address of the user extracted from the subject alternative name), and msUPN (Microsoft User Principal Name). The display names you specified when creating these parameters are displayed on the Create User page when you specify the values for the parameters. For more information, see "Creating Users in Junos Space Network Management Platform" on page 1035.

CAUTION: If you are adding a new parameter with the parameter-based authentication enabled, all users are locked if you activate the parameter without specifying the values of the parameter for all users. This restriction does not apply when you add parameters with the password-based or complete certificate-based authentication mode enabled.

The following topics describe how to add and activate X.509 certificate parameters.

Adding X.509 Certificate Parameters for X.509 Certificate Parameter Authentication

You add X.509 certificate parameters to authenticate users by using X.509 certificate parameters.

To add an X.509 certificate parameter:

1. On the Junos Space Network Management Platform user interface, select **Administration > Applications**.

   The Applications page that appears displays Junos Space Platform and the Junos Space applications installed.

2. Right-click **Network Management Platform** and select **Modify Application Settings**.

   The Modify Application Settings (Modify Network Management Platform Settings) page is displayed and the Device section is selected by default.

3. Click the **X509CertificateParameters** link (on the left of the page) to add the X.509 certificate parameters that are validated during authentication.

   The X509CertificateParameters page that appears displays the X.509 certificate parameters.

Column	Description
Comments	Details about the parameter
Admin Status	Administrative status of the parameter: Activate or Deactivate
Certificate Parameter	Parameter that must be validated during login
Parameter Display Name	Description of the parameter

4. Click the + icon.

   The X509CertificateParameters [New] page is displayed.

5. In the Certificate Parameter field, enter the parameter that must be validated.

6. In the Parameter Display Name field, enter a description about the X.509 certificate parameter.

7. Click **Add**.

8. Repeat steps 3 through 7 to add more parameters that are validated during user login.

9. (Optional) To enter additional comments for a parameter, click the **view/configure** link in the Comments column.

10. (Optional) To deactivate the parameter before enabling authentication using the parameter, click the **Deactivate** link in the Admin Status column.

This step is applicable only if you enabled authentication using parameters and are adding a new parameter.

- To deactivate the parameter, click **Yes** in the Confirmation dialog box.

  The Admin Status column changes to Activate.

- Click **No** to cancel deactivating the parameter.

11. Click **Modify** to save the X.509 certificate parameters.

    You are redirected to the Applications page.

Activating an X.509 Certificate Parameter

If you are authenticating users by using the parameter-based authentication mode and adding a new parameter, you must deactivate the parameter and enter the value of the parameter for all Junos Space Platform users from the Modify User page before activating the parameter for authentication. For more information, refer to "Modifying a User" on page 1044.

To activate an X.509 certificate parameter:

1. On the Junos Space Network Management Platform user interface, select **Administration > Applications > Network Management Platform > Modify Application Settings**.

   The Modify Application Settings (Modify Network Management Platform Settings) page is displayed and the Device section is selected by default.

2. Click the **X509CertificateParameters** link.

   The X509CertificateParameters page that appears displays the X.509 certificate parameters.

3. Select the row corresponding to the certificate parameter you want to activate and click the **Activate** link in the Admin Status column.

   A Confirmation dialog box is displayed.

4. You can activate the parameter or cancel the activation process.

   - To activate the parameter, click **Yes** in the Confirmation dialog box.

     The Admin Status column changes to Deactivate and this parameter is validated during user login.

   - Click **No** to cancel activating the parameter.

5. Click **Modify** to update the modifications.

You are redirected to the Modify Application Settings page.

Release History Table

Release	Description
15.2R1	Starting with Junos Space Network Management Platform Release 15.2R1, you can add X.509 certificate parameters to authenticate users by using X.509 certificate parameters.

RELATED DOCUMENTATION

- Certificate Management Overview | 1426
- Installing a Custom SSL Certificate on the Junos Space Server | 1441
- Modifying an X.509 Certificate Parameter | 1454
- Deleting X.509 Certificate Parameters | 1455

Modifying an X.509 Certificate Parameter

You modify an X.509 certificate parameter to change the parameter used during certificate parameter–based authentication or the display name of the parameter.

CAUTION: If you modify a parameter, you must modify the values of parameters for all users. Users will not be able to log in to Junos Space Platform by using the parameter authentication mode if any of the parameters are modified and their values are not updated for users.

To modify an X.509 certificate parameter:

1. On the Junos Space Network Management Platform user interface, select **Administration > Applications > Network Management Platform > Modify Application Settings**.

   The Modify Application Settings (Modify Network Management Platform Settings) page is displayed and the Device section is selected by default.

2. Click the **X509CertificateParameters** link.

   The X509CertificateParameters page that appears displays the X.509 certificate parameters.

3. Modify the description and name of the parameter.

4. Click **Update** to save the details of the parameter.

5. (Optional) To modify other parameters, click the **X509CertificateParameters** link.

   You are redirected to the X509CertificateParameters page.

6. Repeat steps 2 through 4 to modify the parameters.

7. Click **Modify** to save the details of the parameter.

   You are redirected to the Modify Application Settings page.

RELATED DOCUMENTATION

Adding and Activating X.509 Certificate Parameters for X.509 Certificate Parameter Authentication | **1451**

Deleting X.509 Certificate Parameters | **1455**

Deleting X.509 Certificate Parameters

You delete X.509 certificate parameters to remove them from the list of parameters that are authenticated when a user logs in.

To delete X.509 certificate parameters:

1. On the Junos Space Network Management Platform user interface, select **Administration > Applications > Network Management Platform > Modify Application Settings**.

   The Modify Application Settings (Modify Network Management Platform Settings) page is displayed and the Device section is selected by default.

2. Click the **X509CertificateParameters** link.

   The X509CertificateParameters page that appears displays the X.509 certificate parameters.

3. Select the rows corresponding to the certificate parameters you want to delete and click the - icon (on the left of the page).

   A Confirmation dialog box is displayed.

4. You can delete the parameter or retain the parameter in Junos Space Platform.

   - To delete the parameters, click **Yes** in the Confirmation dialog box.

     The selected X.509 certificate parameters are deleted.

   - Click **No** to retain the parameters.

5. Click **Modify** to save the modifications to the list of parameters.

   You are redirected to the Modify Application Settings page.

RELATED DOCUMENTATION

Adding and Activating X.509 Certificate Parameters for X.509 Certificate Parameter Authentication | **1451**

Modifying an X.509 Certificate Parameter | **1454**

CHAPTER 75

Configuring Authentication Servers

IN THIS CHAPTER

- Remote Authentication Overview | 1457
- Junos Space Authentication Modes Overview | 1458
- Junos Space Login Behavior with Remote Authentication Enabled | 1461
- Managing Remote Authentication Servers | 1467
- Creating a Remote Authentication Server | 1468
- Modifying Authentication Settings | 1471
- Configuring a RADIUS Server for Authentication and Authorization | 1473
- Configuring a TACACS+ Server for Authentication and Authorization | 1475

Remote Authentication Overview

Junos Space Network Management Platform, by default, authenticates users to log in locally when you configure their accounts by using **Role Based Access Control** > **User Accounts** > **Create User** (icon) task.

On the **Administration** > **Authentication Servers** inventory landing page, you can authenticate users to log in exclusively from a centralized location by using one or more RADIUS or TACACS+ remote authentication servers. You can also authenticate users to log in to Junos Space Network Management Platform by using both local and remote authentication.

You can configure the order in which Junos Space Network Management Platform connects to remote authentication servers by preference. Junos Space Network Management Platform authenticates users by using the first reachable remote authentication server on the list.

Junos Space Network Management Platform supports the following RADIUS authentication methods: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2). For TACACS+ authentication, Junos Space Platform supports Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

> **NOTE:** If you configure remote authentication using RADIUS or TACACS+, then the most restrictive concurrent session limit between the Junos Space server and the remote authentication server takes effect.

You must have Super Administrator or System Administrator privileges to configure remote authentication server settings, authentication modes, and user passwords and settings.

Regular Junos Space Network Management Platform users cannot configure their own passwords if you maintain users solely by using a remote authentication server. You may choose to allow some privileged users to set a local password so they can still log in to Junos Space if the remote authentication server is unreachable.

RELATED DOCUMENTATION

- Configuring User Access Controls Overview | 69
- Junos Space Authentication Modes Overview | 1458
- Managing Remote Authentication Servers | 1467
- Creating a Remote Authentication Server | 1468
- Configuring a RADIUS Server for Authentication and Authorization | 1473
- Configuring a TACACS+ Server for Authentication and Authorization | 1475
- Modifying Authentication Settings | 1471
- Junos Space Login Behavior with Remote Authentication Enabled | 1461

Junos Space Authentication Modes Overview

IN THIS SECTION

- Local Authentication | 1459
- Remote Authentication | 1459
- Remote-Local Authentication | 1460

Junos Space Network Management Platform provides three authentication modes: local, remote, and remote-local. The default authentication mode is local.

For each of these modes, authentication and authorization is performed in the following ways:

- Local—Authentication and authorization are performed by Junos Space Platform based on the user account and role information in the Junos Space database. You can create the user account for local authentication from the **Role Based Access Control** > **User Accounts** task.
- Remote—Authentication and authorization are performed by a set of remote AAA servers (RADIUS or TACACS+). You can configure remote authentication from the **Administration** > **Authentication Servers** task.
- Remote-Local—When a user is not configured on the remote authentication servers or when the servers are unreachable, the local password and role information are used if such a local user exists in the Junos Space database. You can configure remote-local authentication from the **Administration** > **Authentication Servers** task.

The following sections describe the authentication modes:

Local Authentication

The user is authenticated and authorized using the local Junos Space Network Management Platform database. By default, Junos Space Platform authenticates users locally. Before you can authenticate a user by using local authentication mode, you must create the user account in Junos Space Platform with a valid password and assign roles to the user. To create a user account in Junos Space Platform, use the **Role Based Access Control** >**User Accounts** > **Create User** (icon) task.

For more information, see the "Configuring Users to Manage Objects in Junos Space Overview" on page 1033, "Creating Users in Junos Space Network Management Platform" on page 1035, and "Creating a User-Defined Role" on page 1022 topics.

Remote Authentication

User authentication information is stored on one or more remote authentication servers. Authorization information can also be configured and stored on the remote authentication server. To configure Junos Space Network Management Platform remote authentication, see "Managing Remote Authentication Servers" on page 1467.

In this mode, if a corresponding local user exists, the local password is used only in the emergency case where the authentication servers are unreachable.

Before you authenticate and authorize users by using remote authentication mode, you must make sure that:

- You create and configure the remote authentication server in Junos Space Platform (see "Creating a Remote Authentication Server" on page 1468).
- You create the remote profiles required for authorizing the users in Junos Space Platform (see "Creating a Remote Profile" on page 1098).
- You configure the RADIUS or TACACS+ server for authentication and authorization of users (see "Configuring a RADIUS Server for Authentication and Authorization" on page 1473 or "Configuring a TACACS+ Server for Authentication and Authorization" on page 1475).
- You create the user accounts by using the **Role Based Access Control** workspace in Junos Space Platform if you want to permit local authentication and authorization for select users when the remote authentication servers are not reachable (see "Creating Users in Junos Space Network Management Platform" on page 1035).

Remote-Local Authentication

User authentication information is stored on one or more remote authentication servers. Authorization information can also be configured and stored on the remote authentication server. For more information about configuring Junos Space Network Management Platform remote-local authentication, see "Managing Remote Authentication Servers" on page 1467.

In this mode, when a user is not configured on the remote authentication server, when the server is unreachable, or when the remote server denies the user access, then the local password is used if such a local user exists in the Junos Space Network Management Platform database.

Before you authenticate and authorize users by using remote-local authentication mode, you must make sure that:

- You create and configure the remote authentication server in Junos Space Platform (see "Creating a Remote Authentication Server" on page 1468).
- You create the remote profiles required for authorizing the users in Junos Space Platform (see "Creating a Remote Profile" on page 1098).
- You configure the RADIUS or TACACS+ server for authentication and authorization of users (see "Configuring a RADIUS Server for Authentication and Authorization" on page 1473 or "Configuring a TACACS+ Server for Authentication and Authorization" on page 1475).
- You create user accounts by using the **Role Based Access Control** workspace in Junos Space Platform to permit local authentication and authorization (see "Creating Users in Junos Space Network Management Platform" on page 1035).

RELATED DOCUMENTATION

Configuring User Access Controls Overview | 69
Remote Authentication Overview | 1457
Configuring a RADIUS Server for Authentication and Authorization | 1473
Configuring a TACACS+ Server for Authentication and Authorization | 1475
Managing Remote Authentication Servers | 1467
Creating a Remote Authentication Server | 1468
Modifying Authentication Settings | 1471

Junos Space Login Behavior with Remote Authentication Enabled

This topic describes the Junos Space Network Management Platform login behavior with remote authentication only or remote-local authentication enabled.

WARNING: To avoid a BEAST TLS 1.0 attack, whenever you log in to Junos Space Network Management Platform in a browser tab or window, make sure that tab or window was not previously used to surf a non-HTTPS website. Best practice is to close your browser and relaunch it before logging in to Junos Space Platform.

System behavior differs depending on whether you select remote authentication only or remote-local authentication as the authentication mode for Junos Space Platform. Differences occur when a remote authentication server does not authenticate a user. There are also differences in the source of authorization depending on what answer the remote server returns.

Figure 140 shows the decision tree underlying system behavior when either remote authentication only or remote-local authentication is chosen and a remote authentication server accepts the user.

Figure 140: Remote Authentication Server Accepts User

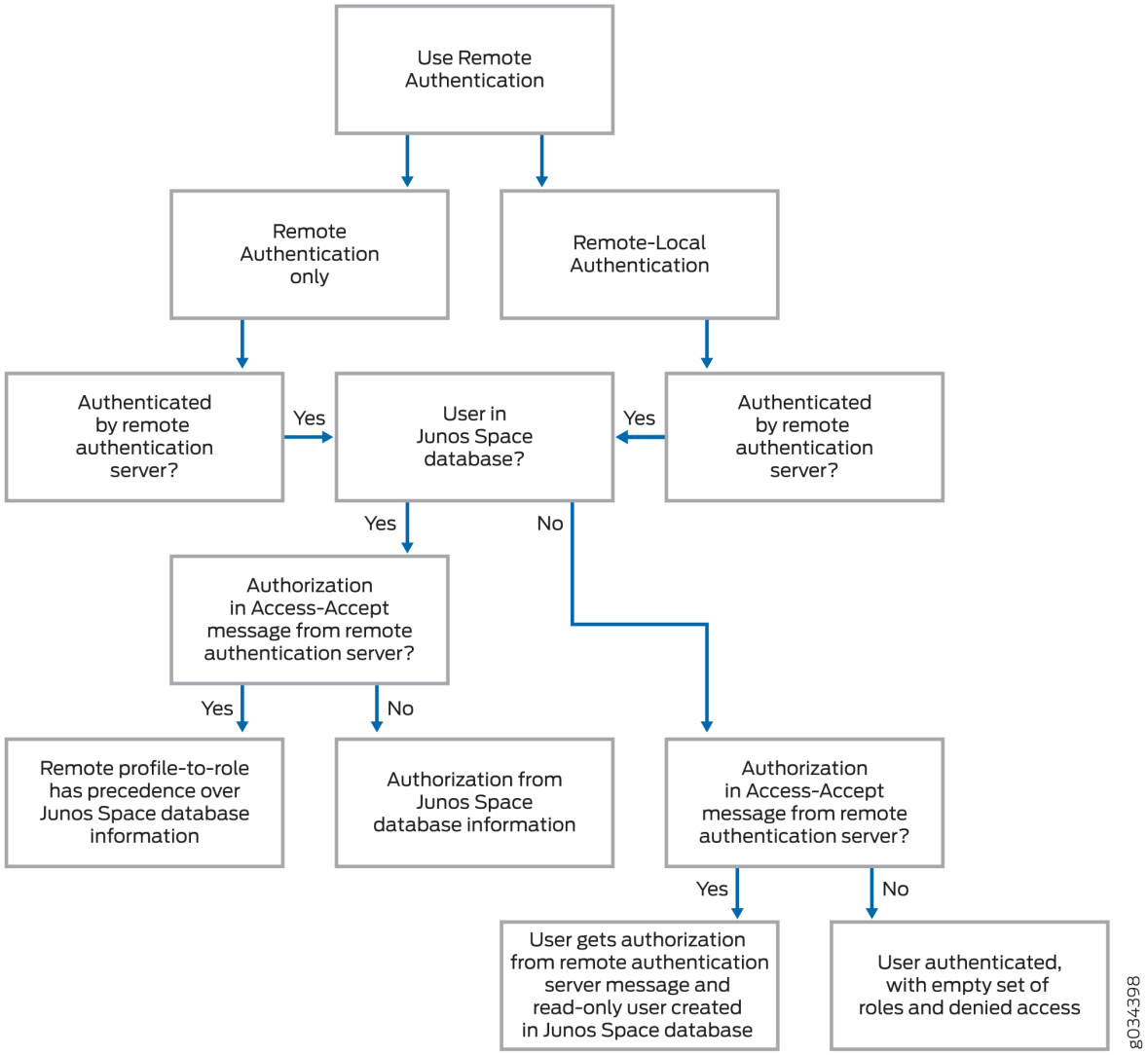
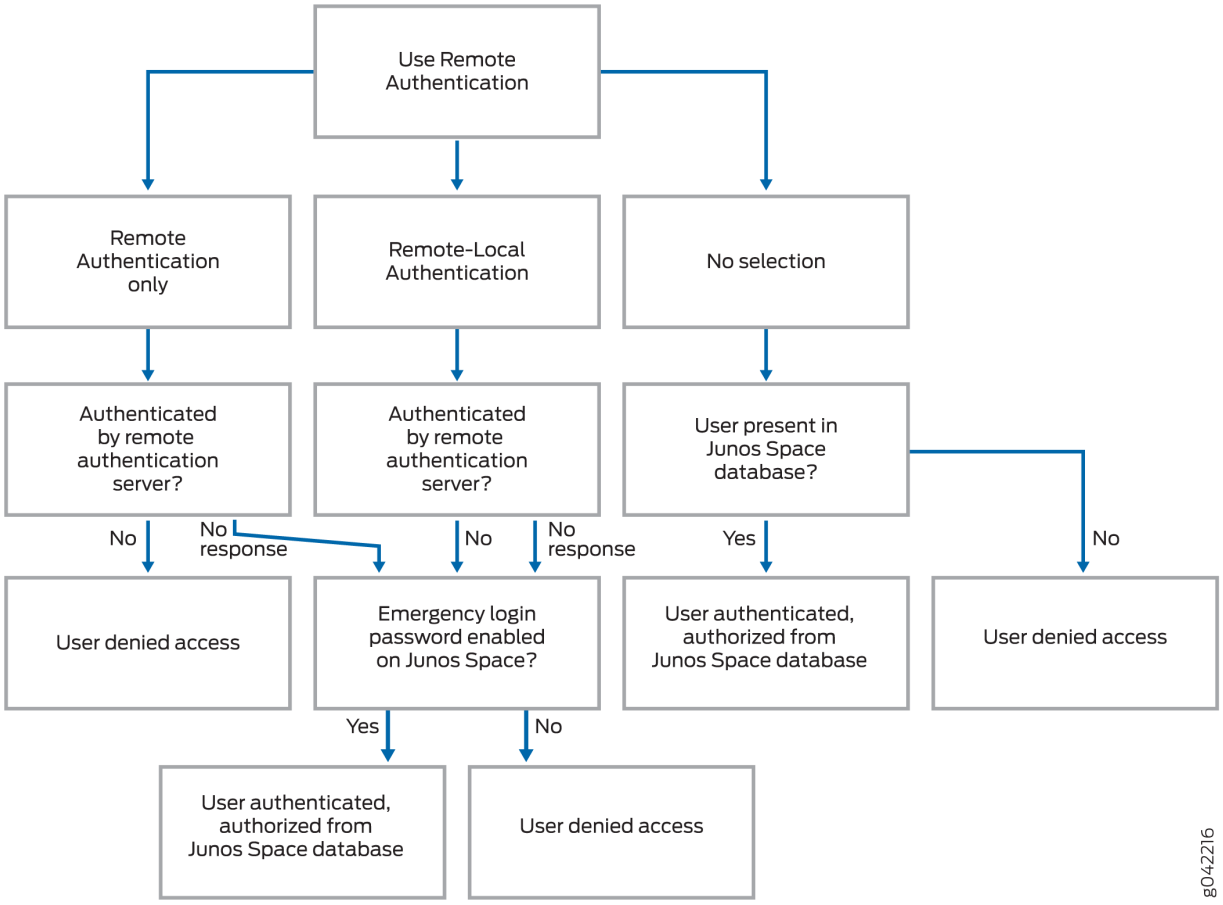


Figure 141 shows the decision tree when a remote authentication server either rejects the user or does not respond at all.

Figure 141: Remote Authentication Server Not Reachable or Rejects User



The following sections describe the login behavior when remote authentication only or remote-local authentication mode is enabled.

NOTE: When remote users log in with usernames that contain an @ symbol or a backslash (\) character, Junos Space Platform ignores the part of the username that follows the @ symbol or the part that precedes the backslash character and authenticates with the rest of the username. For example, if a remote user uses *abc@domain*, *abc@domain.com*, or *domain\abc* as the username, Junos Space Platform uses only *abc* to authenticate the user. If there is an entry for *abc* in the database, the corresponding remote profile is applied to the user. If the database does not have an entry that corresponds to the username, *abc* in the given example, Junos Space Platform creates a read-only user account with the name abc and assigns a remote profile.

Login Behavior with Remote Authentication Only Enabled

Table 185 lists the various scenarios and the authentication and authorization behavior for each scenario when remote authentication only mode is enabled.

Table 185: Login Behavior with Remote Authentication Only Enabled

Scenario	Login Behavior
User logs in with the correct credentials	• If the user's password is on the remote server and there is a corresponding remote profile in Junos Space Platform, the user logs in with the roles assigned by the remote profile. • If the user's password is on the remote server but there is no equivalent remote profile in Junos Space Platform, the user logs in with roles assigned from the Junos Space database user information if the corresponding user account exists in the Junos Space database. If there is no equivalent remote profile or user account in Junos Space Platform, the user is denied access. • If the first remote authentication server is present, only that server is contacted and login success or failure solely depends on the password stored there. If the first authentication server is not reachable, the other servers are contacted in the specified order. If no authentication server is reachable, the local password in the Junos Space Platform database is checked. If the emergency password is configured in Junos Space and the credentials match, the user logs in successfully with roles assigned from the Junos Space database user information. Otherwise, the user is denied access. **NOTE:** For remote authentication and authorization, most users do not need a local password. The local password in this case is only for emergency purposes, when the remote authentication servers are unreachable.
User logs in with incorrect credentials or the user does not exist on the remote authentication server	• Access to Junos Space Platform is denied. **NOTE:** Authentication servers, for security purposes, do not distinguish between these two cases (that is, a user is logging in with incorrect credentials or a user does not exist on the remote authentication server). Therefore, Junos Space Platform must always treat these type of logins as an authentication failure. • If no authentication servers are reachable, Junos Space Platform tries the local password. If the emergency password is configured in Junos Space and the credentials match, the user logs in successfully with roles assigned from the Junos Space database user information. Otherwise, the user is denied access.

Table 185: Login Behavior with Remote Authentication Only Enabled *(continued)*

Scenario	Login Behavior
User attempts to log in when the remote authentication server is configured for Challenge/Response	• If the remote authentication server indicates that a challenge is required, it provides the challenge question. Junos Space Platform displays the challenge question to the user on the Junos Space login page and waits for the user's response. • If the challenge question is answered correctly, it is possible that the authentication server may pose additional challenge questions. • If the challenge question is answered incorrectly, it is possible that the authentication server may rechallenge the user with the same challenge question, use a different challenge question, or fail the login attempt completely. The remote authentication server configuration determines the behavior. • If the final challenge question is answered correctly, the user logs in successfully.

Login Behavior with Remote-Local Authentication Enabled

Table 186 lists the various scenarios and the authentication and authorization behavior for each scenario when the remote-local authentication mode is enabled.

Table 186: Login Behavior with Remote-Local Authentication Enabled

Scenario	Login Behavior
User logs in with the correct credentials	• If the user's password is on the remote server and there is a corresponding remote profile in Junos Space Platform, the user logs in with the roles assigned by the remote profile. • If the user's password is on the remote server, but there is no equivalent remote profile in Junos Space database, then Junos Space Platform checks whether the user account exists in the Junos Space database. If the user account exists, the user logs in successfully with the roles assigned from the Junos Space database user information. Otherwise, the user is denied access. • If the remote servers are not reachable, Junos Space Platform tries to authenticate the user locally. If a Junos Space Platform user account and local password exist, and the credentials match, the user logs in successfully with the roles assigned from the Junos Space database user information. Otherwise, the user is denied access.
User logs in with incorrect credentials or the user does not exist on the remote authentication server	• Junos Space Platform checks the remote authentication servers first. If authentication fails or if a server is not reachable, Junos Space Platform tries to authenticate the user locally. If a Junos Space Platform user account and local password exist, and the credentials match, the user logs in successfully with the roles assigned from the Junos Space database user information. Otherwise, the user is denied access.

Table 186: Login Behavior with Remote-Local Authentication Enabled *(continued)*

Scenario	Login Behavior
User attempts to log in when the remote authentication server is configured for Challenge/Response	• If the remote authentication server indicates that a challenge is required, it provides the challenge question. Junos Space Platform displays the challenge question to the user on the Junos Space login page and waits for the user's response. • If the challenge question is answered correctly, it is possible that the authentication server may pose additional challenge questions. • If the challenge question is answered incorrectly, it is possible that the authentication server may rechallenge the user with the same challenge question, use a different challenge question, or fail the login attempt completely. The remote authentication server configuration determines the behavior. • If the final challenge question is answered correctly, the user logs in successfully.

RELATED DOCUMENTATION

- Remote Authentication Overview | 1457
- Logging In to Junos Space | 100
- Junos Space Authentication Modes Overview | 1458
- Creating a Remote Authentication Server | 1468
- Modifying Authentication Settings | 1471

Managing Remote Authentication Servers

The **Administration** > **Authentication Servers** page allows you to configure remote authentication settings to allow users to log in to Junos Space Network Management Platform from a remote authentication server. The **Authentication Servers** page includes two areas: **Authentication Mode Setting** and **Remote Authentication Servers** table.

From the **Authentication Mode Setting** area, you can select and save the Junos Space Network Management Platform authentication mode: local, remote, or remote-local.

From the **Remote Authentication Servers** table area, you can:

- Create, modify, and delete remote authentication server connection settings and test the connection.
- Specify the remote authentication server connection order.

To select the remote authentication mode and manage remote authentication servers:

1. Select **Administration** > **Authentication Servers**.

2. In the **Authentication Mode Setting** area, select the authentication method you want to use.

   By default, Junos Space Network Management Platform is in local authentication mode and the controls for the **Remote Authentication Servers** table are disabled. If you select the **Use Remote Authentication** check box, the **Remote Authentication Only** and **Remote-Local Authentication** options are enabled.

3. Click **Save** to store the remote authentication mode setting you select.

4. In the **Remote Authentication Servers** table, add a new remote authentication server by clicking the **Add auth server** (**+**) icon. See "Creating a Remote Authentication Server" on page 1468.

5. Modify an authentication server by doubling clicking that server row in the table. See "Modifying Authentication Settings" on page 1471.

6. Delete an authentication server by selecting a row and clicking the **Delete auth server** (**–**) icon to remove an authentication server.

7. Click a row and select the arrows to move the server up and down the list. Up arrow is disabled if the server is at the top of the list; down arrow is disabled if the server is at the bottom of the list.

   Sorting for columns are disabled, since there is an explicit sort order as determined by the arrows.

8. On selection of the server, click **Test Connection** to display a transient result of last connection test.

9. Confirm that you want to test the server connection.

After testing, the Status dialog box appears displaying the test results: success or failure.

10. Click **OK**.

    If the connection results fails, ensure that the server settings are correct.

RELATED DOCUMENTATION

- Remote Authentication Overview | **1457**
- Junos Space Authentication Modes Overview | **1458**
- Creating a Remote Authentication Server | **1468**
- Modifying Authentication Settings | **1471**
- Junos Space Login Behavior with Remote Authentication Enabled | **1461**

Creating a Remote Authentication Server

To run Junos Space Network Management Platform remote authentication, you must create one or more remote authentication servers and configure the server settings.

To create a remote authentication server:

1. Select **Administration** > **Authentication Servers**.

   The Authentication Servers page is displayed.

2. (Optional) If you want to use one of the remote authentication modes supported by Junos Space Platform, in the **Authentication Mode Setting** area, perform the following tasks:

   NOTE: Junos Space Platform allows you to add authentication servers even when you are using local authentication. This enables you to configure the authentication server settings *before* enabling and specifying a remote authentication mode.

   a. Select the **Use Remote Authentication** check box.

      The option button to specify the remote authentication mode is enabled.

   b. Specify the remote authentication mode that you want to use. Do one of the following:

      - Select **Remote Authentication Only** to use the remote authentication mode supported by Junos Space Platform.

- Select **Remote-Local Authentication** to use the remote local authentication mode supported by Junos Space Platform.

c. Click **Save** to store the remote authentication mode setting you select.

3. To add a remote authentication server:

a. Click the **+** (**Add auth server**) icon.

The Create Auth Server dialog box is displayed.

b. Specify the remote authentication server fields, as explained in Table 187; all the fields are mandatory.

Table 187: Remote Authentication Server Parameters

Parameter	Description
Server Type	Specify the type of the authentication server: • **RADIUS**—Authenticate users by using a RADIUS server. • **TACACS+**—Authenticate users by using a TACACS+ server.
Server Name	Specify the name of the remote authentication server. The remote authentication server name cannot exceed 128 characters and can contain only letters, numbers, hyphens, underscores, or periods.
Protocol	Select one of the following authentication protocols supported by the remote server: • **PAP**—Password Authentication Protocol • **CHAP**—Challenge Handshake Authentication Protocol • **MS-CHAPv2**—(RADIUS only) Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2)
IP Address	Specify the IP address of the remote authentication server. **NOTE:** • Depending on whether the Junos Space fabric is configured with only IPv4 addresses or both IPv4 and IPv6 addresses, Junos Space Platform allows you to enter an IPv4 address or either an IPv4 or IPv6 address respectively for the remote authentication server. • The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to http://www.iana.org/assignments/ipv4-address-space for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space for the list of restricted IPv6 addresses.
Port Number	Specify the UDP port number assigned by the remote authentication server. The default port number is 1812 for RADIUS authentication and 49 for TACACS+ authentication.

Table 187: Remote Authentication Server Parameters *(continued)*

Parameter	Description
Shared Secret	Specify the password (shared secret) that is used for authentication between the remote authentication server, the proxy authentication server, and Junos Space Platform. The shared secret that you specify must match the shared secret configured in the RADIUS or TACACS+ server.
Confirm Shared Secret	Reenter the password (shared secret) to confirm.
Number of Tries	Specify the number of retries that a Junos Space Platform attempts to contact the remote authentication server. After the specified number of tries is exceeded and if you have configured other servers, Junos Space Platform attempts to contact the other authentication servers one by one. You can enter a value from 1 through 5; the default is 3 tries.
Max Retry Timeout MSecs	Specify the interval (in milliseconds) that the Junos Space Platform waits for a reply from the remote authentication server before it times out. The minimum value is 1000 milliseconds and the default is 6000 milliseconds.

c. Click **OK**.

The remote authentication server is created and displayed in the table on the Authentication Servers page.

4. (Optional) Click **Test Connection** to verify the connection from Junos Space Platform to the remote authentication server.
   - If the test connection result is a success, the remote authentication server is reachable.
   - If the test connection result is a failure, the remote authentication server is unreachable.
   - If the test connection result displays the message *Mismatched shared secret*, then the configured shared secret for that server is incorrect. Ensure that you have entered the correct remote authentication server shared secret details.

RELATED DOCUMENTATION

Configuring a RADIUS Server for Authentication and Authorization | 1473

Configuring a TACACS+ Server for Authentication and Authorization | 1475
Remote Authentication Overview | 1457
Junos Space Authentication Modes Overview | 1458
Modifying Authentication Settings | 1471
Configuring a RADIUS Server for Authentication and Authorization | 1473

Modifying Authentication Settings

The Authentication Servers page allows you to change Junos Space Network Management Platform authentication mode and remote authentication server connection settings.

To modify remote authentication settings:

1. Select **Administration > Authentication Servers**.

   The Authentication Servers page appears.

2. In the **Authentication Mode Setting** area, change to the authentication method you want to use.

   By default, Junos Space Network Management Platform is in local authentication mode and the controls for the Remote Authentication Servers table are disabled. If you select the **Use Remote Authentication** check box, the **Remote Authentication Only** and **Remote-Local Authentication** options are enabled.

3. To modify the authentication mode settings, in the **Authentication Mode Setting** area, perform one of the following tasks:

   - Clear the **Use Remote Authentication** check box to use local authentication
   - Select the **Use Remote Authentication** check box to use remote authentication.

     The option button to specify the remote authentication mode is enabled. Perform one of the following tasks:

     - Select **Remote Authentication Only** to use the remote authentication mode supported by Junos Space Platform.
     - Select **Remote-Local Authentication** to use the remote local authentication mode supported by Junos Space Platform.

   - Click **Save** to store the remote authentication mode setting you select.

4. To modify a previously configured remote authentication server:

   a. Select the authentication server that you want to modify.

      The authentication server that you selected is highlighted.

b. Click the pencil icon corresponding to the authentication server you selected.

   The previously configured parameters are displayed below the authentication server that you selected. You can modify all the configured parameters except the name of the authentication server. For more details, see the "Creating a Remote Authentication Server" on page 1468 topic.

c. After you have modified the authentication server settings, click **OK**.

   The modifications that you made are saved.

5. (Optional) Click **Test Connection** to verify the connection from Junos Space Platform to the remote authentication server.

   - If the test connection result is a success, the remote authentication server is reachable.
   - If the test connection result is a failure, the remote authentication server is unreachable.
   - If the test connection result displays the message *Mismatched shared secret*, then the configured shared secret for that server is incorrect. Ensure that you have entered the correct remote authentication server shared secret details.

RELATED DOCUMENTATION

Remote Authentication Overview | **1457**

Junos Space Authentication Modes Overview | **1458**

Creating a Remote Authentication Server | **1468**

Managing Remote Authentication Servers | **1467**

Junos Space Login Behavior with Remote Authentication Enabled | **1461**

Configuring a RADIUS Server for Authentication and Authorization

Junos Space Network Management Platform supports authorization of users from a RADIUS server. Using the Authentication Servers page (**Administration** > **Authentication Servers**), you can configure a RADIUS server to authenticate and authorize users to log in exclusively from a centralized location using one or more RADIUS remote authentication servers. You can also authenticate and authorize users to log in to Junos Space Platform using both local and remote authentication and authorization.

NOTE: Before you authenticate and authorize users to login to Junos Space Platform by using the RADIUS server, you must make sure that:

- You create and configure the RADIUS remote authentication server in Junos Space Platform (see "Creating a Remote Authentication Server" on page 1468).
- You create the remote profiles required for authorizing the users in Junos Space Platform (see "Creating a Remote Profile" on page 1098).
- You create user accounts by using the **Role Based Access Control** workspace in Junos Space Platform if you want to permit remote authentication and local authorization (see "Creating Users in Junos Space Network Management Platform" on page 1035).

To understand login behavior with remote authentication enabled, see the "Junos Space Login Behavior with Remote Authentication Enabled" on page 1461 topic.

Authorization data in the RADIUS server are stored as vendor-specific attributes (VSAs). Therefore, you must update the Junos dictionary file (**juniper.dct**) in the RADIUS server with the Junos Space Platform defined VSA (*Juniper-Junosspace-Profiles*). Users in the RADIUS server database should be assigned the VSA with the value corresponding to the Junos Space remote profile that you want to assign to the user. The user is authorized with roles specified by the remote profile. For a list of relevant Juniper RADIUS VSAs, see Juniper Networks Vendor-Specific RADIUS Attributes.

To configure VSAs in Steel-Belted Radius:

1. Add the Junos Space VSA to the Juniper dictionary file (**juniper.dct**). Locate the dictionary file and add the following text to the file:

   ```
   ATTRIBUTE Juniper-Junosspace-Profiles Juniper-VSA(11, string) r
   ```

2. Assign a remote profile to the user by using the *Juniper-Junosspace-Profiles* attribute.

   For more information about adding the VSA and assigning a Junos Space remote profile to a user in Steel-Belted RADIUS, see the Steel-Belted RADIUS documentation.

To configure VSAs in FreeRADIUS:

1. Add the Junos Space VSA to the Juniper dictionary file (**dictionary.juniper**). Locate the dictionary file and add the following text to the file:

   ```
   ATTRIBUTE Juniper-Junosspace-Profiles 11 String
   ```

2. Assign a remote profile to the user by using the *Juniper-Junosspace-Profiles* attribute.

   The following example shows how configuration information can be added to FreeRADIUS to assign a remote profile to a user:

   ```
   "guestuser" Auth-Type:=PAP, User-Password:="<password>"
   Juniper-Junosspace-Profiles = "guestprofile"
   ```

   For more information about adding the VSA and assigning a Junos Space remote profile to a user in Free RADIUS, see the FreeRADIUS documentation.

> **NOTE:** The remote profiles created in Junos Space Platform are not automatically synchronized to the RADIUS server for selection. The administrator must manually enter the correct remote profile name.

RELATED DOCUMENTATION

- Remote Authentication Overview | **1457**
- Junos Space Authentication Modes Overview | **1458**
- Managing Remote Authentication Servers | **1467**
- Creating a Remote Authentication Server | **1468**
- Modifying Authentication Settings | **1471**
- Configuring a TACACS+ Server for Authentication and Authorization | **1475**
- Junos Space Login Behavior with Remote Authentication Enabled | **1461**

Configuring a TACACS+ Server for Authentication and Authorization

Junos Space Network Management Platform supports authentication and authorization of users from one or more TACACS+ servers. (A combination of TACACS+ and RADIUS servers is also supported.) If you configure multiple servers, they will be tried during authentication in the order listed in the user interface. If the first server accessed is not reachable or there is a shared-secret mismatch, the next one is tried. To understand login behavior with remote authentication enabled, see the "Junos Space Login Behavior with Remote Authentication Enabled" on page 1461 topic.

> **NOTE:** Before you authenticate and authorize users to log into Junos Space Platform by using the TACACS+ server, you must make sure that:
>
> - You create and configure the TACACS+ remote authentication server in Junos Space Platform (see "Creating a Remote Authentication Server" on page 1468).
> - You create the remote profiles required for authorizing the users in Junos Space Platform (see "Creating a Remote Profile" on page 1098).
> - You create user accounts by using the **Role Based Access Control** workspace in Junos Space Platform if you want to permit remote authentication and local authorization (see "Creating Users in Junos Space Network Management Platform" on page 1035).

Authorization data in the TACACS+ server are stored as attribute-value pairs (AVPs). The AVP contains the name of the remote profile. Therefore, you must configure users in the TACACS+ server with the AVPs corresponding to the remote profiles created in the Junos Space server to represent the user's roles.

When Junos Space Network Management Platform queries the TACACS+ server for user authorization, the TACACS+ server's junosspace-exec service returns the remote profile name for that user. Junos Space Network Management Platform determines the user's role or roles from this response.

To assign roles to the user using the remote profile name, you can configure the network-management-profiles AVP for the junosspace-exec service on the TACACS+ server.

The following example shows how configuration information can be added to the TACACS+ server to assign a remote profile to a user:

```
user = guestuser
{
 pap = cleartext "<password>"
 service = junosspace-exec
 {
  network-management-profiles = guest_profile
```

```
 }
}
```

For more information about configuring the AVP and assigning a Junos Space remote profile to a user in the TACACS+ server, see the TACACS+ server documentation.

RELATED DOCUMENTATION

- Remote Authentication Overview | **1457**
- Junos Space Authentication Modes Overview | **1458**
- Managing Remote Authentication Servers | **1467**
- Creating a Remote Authentication Server | **1468**
- Modifying Authentication Settings | **1471**
- Configuring a RADIUS Server for Authentication and Authorization | **1473**
- Junos Space Login Behavior with Remote Authentication Enabled | **1461**

CHAPTER 76

Managing SMTP Servers

IN THIS CHAPTER

- Managing SMTP Servers | 1477
- Adding an SMTP Server | 1478

Managing SMTP Servers

You can configure one or several SMTP servers for use by Junos Space applications that need to transmit e-mail. For example, an application might use e-mail automatically to inform a support organization of an issue and might include logs or reports.

To configure and manage SMTP servers:

1. Select **Administration** > **SMTP Servers**.

   The SMTP Servers page appears listing all the configured servers. Only one server can be the active server at one time. The active server is highlighted.

To add or delete an SMTP server:

1. Click the plus sign (**Add SMTP server** icon) at the upper left of the page to add a server.
2. Configure and add the server. See "Adding an SMTP Server" on page 1478.
3. To delete a server, click the – sign (**Delete SMTP server** icon) at the upper left of the page.

   NOTE: If you try to delete the active SMTP server, an error message is displayed indicating that you cannot delete the server.

To change the active SMTP server:

- Click the **Set Active SMTP server** icon at the upper left of the page to select the server you want to make active. Click **Yes** on the confirmation message that appears to set the selected server as the active SMTP server. If there is only one server and it is the active server, clicking **No** on the confirmation message has no effect.

The Test connection settings option is used to test the SMTP server connection from Junos Space Network Management Platform. This option uses the user-defined (selected), authentication, and security details when it tests the connection between the SMTP server and Junos Space Network Management Platform. To test the connection to the server:

- Click the **Test Connection** button at the upper-right corner of the page.

  If the SMTP server supports only the TLS security protocol, the connectivity test succeeds for both the None and TLS security options. This is a known limitation in the connectivity test for testing the connection between the SMTP server and Junos Space Network Management Platform.

RELATED DOCUMENTATION

Adding an SMTP Server | **1478**

Adding an SMTP Server

You can add an SMTP server to the list of configured servers to which applications can direct e-mail. To add an SMTP server, you must have administration privileges.

To add an SMTP server:

1. Select **Administration** > **SMTP Servers**.

   The SMTP Servers page appears displaying the list of SMTP servers already configured.

2. Click the plus (+) icon (**Add SMTP Server**) in the upper-left corner.

   The Create SMTP Server dialog box appears.

3. In the **Server Name** text box, enter a name for the SMTP server, using alphanumeric values.

   The SMTP server name cannot exceed 128 characters. The name can contain only letters and numbers and can include a hyphen (-), underscore (_), or period (.).

4. In the **Host Address** text box, enter the IP address or the hostname of the SMTP server.

The IP address or the hostname that you enter should be valid and should not contain any special characters.

NOTE:

- Depending on whether the Junos Space fabric is configured with only IPv4 addresses or both IPv4 and IPv6 addresses, Junos Space Platform allows you to enter an IPv4 address or either an IPv4 or IPv6 address respectively for the SMTP server.
- The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to http://www.iana.org/assignments/ipv4-address-space for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space for the list of restricted IPv6 addresses.

5. Enter the port number in the **Port Number** text box

   The default port number is 587.

6. In the **From Email Address** text box, enter the e-mail address of this server in the format: *user@example*.com.

   This address appears as the sender of e-mail message from the applications that are using this server.

7. Select the **Set As Active Server** check box to set this server as the primary or active SMTP server. All applications then redirect the e-mail message to this SMTP server.

8. (Optional) If you want to use the SMTP Authentication security protocol to check the credentials of the sender, select **Use SMTP Authentication**.

   When you select this option, the related **User Name**, **Password**, **Confirm Password**, and **Security** fields are enabled.

   Enter the following information related to SMTP authentication:

   a. In the **User Name** text box, enter the username that you want to use for authentication.

   b. Enter the authentication password in the **Password** and **Confirm Password** text boxes.

   c. (Optional) If you want to use Transport Layer Security (TLS) or Secure Sockets Layer (SSL) for further protection, select **TLS** or **SSL** from the **Security** list.

      By default, no security protocol (**None**) is used.

9. Click **Save**.

   The SMTP server that you added is saved and displayed in the STMP Servers page.

RELATED DOCUMENTATION

Managing SMTP Servers | 1477

CHAPTER 77

Email Listeners

IN THIS CHAPTER

- Email Listeners Overview | 1481
- Adding Users to the Email Listeners List | 1482
- Modifying Users in the Email Listeners List | 1483
- Deleting Users from the Email Listeners List | 1484

Email Listeners Overview

The Email Listeners list is a list that contains e-mail addresses of users who receive notifications about the health of the Junos Space system through a System Health Report from Junos Space Network Management Platform. To this list, you can add e-mail addresses of users who are Junos Space users and e-mail addresses that are not added to the Junos Space Platform database. You can edit or delete the details in the Email Listeners list.

Users added as E-mail Listeners receive notifications when an issue occurs (Status column displays a red Yes) and when an issue is fixed (Status column displays a red No) for all parameters in the System Health Report (with the exception of HPROF availability and JBoss restart observed in the preceding three days). For more information about the parameters in the System Health Report, refer to "Viewing the Administration Statistics" on page 1138.

For an Email Listener to receive e-mail notifications, the active SMTP server must be reachable from Junos Space Platform. For more information about configuring an SMTP server, refer to "Adding an SMTP Server" on page 1478. Your role must be assigned the required privileges to add, modify, or delete users from the Email Listeners list.

RELATED DOCUMENTATION

- Adding Users to the Email Listeners List | 1482
- Deleting Users from the Email Listeners List | 1484
- Modifying Users in the Email Listeners List | 1483

Adding Users to the Email Listeners List

You add users to the Email Listeners list if they must receive notifications about the health of the system through a System Health Report from Junos Space Network Management Platform. You can add e-mail addresses of users who are not added to the Junos Space Platform database.

> **NOTE:** For a user to receive e-mail notifications, the active SMTP server must be reachable from Junos Space Platform. Your role must be assigned the required privileges so that you can add users to the Email Listeners list.

To add a user to the Email Listeners list:

1. On the Junos Space Network Management Platform user interface, select **Administration > Email Listeners**.

   The Email Listeners page that appears displays the list of users who receive notifications about the health of the system.

2. Click the Create Email Listener icon (on the right of the page).

   The Create Email Listener pop-up window is displayed.

   > **NOTE:** If you have not configured an active SMTP server, the following error message is displayed: **No active SMTP server configured, please go to Administration -> SMTP Servers to configure it.**

3. From the **Type of Notification** drop-down list, select Fabric Health Monitoring.

4. In the **Email ID** field, enter the e-mail address of the user who should receive notifications.

5. (Optional) In the **Description** field, add a description about the e-mail listener.

6. Click **Save**.

   The user's e-mail address is added to the Email Listeners list.

RELATED DOCUMENTATION

Modifying Users in the Email Listeners List | 1483
Viewing the Administration Statistics | 1138
Adding an SMTP Server | 1478
Modifying Junos Space Network Management Platform Settings | 1346
Deleting Users from the Email Listeners List | 1484

Modifying Users in the Email Listeners List

If a user's e-mail address has changed, you need to modify the details of the user in the Email Listeners list so that notifications can be sent to the new e-mail address.

> **NOTE:** Your role must be assigned the required privileges so that you can modify the details of users in the Email Listeners list.

To modify the details of a user in the Email Listeners list:

1. On the Junos Space Network Management Platform user interface, select **Administration > Email Listeners**.

   The Email Listeners page that appears displays the list of users who receive notifications about the health of the system.

2. Select the Pencil icon corresponding to the user whose details must be modified.

3. In the **Email ID** field, modify the e-mail address.

4. In the **Description** field, modify the description.

5. Click **Save** to save the changes.

RELATED DOCUMENTATION

Adding Users to the Email Listeners List | 1482
Deleting Users from the Email Listeners List | 1484

Deleting Users from the Email Listeners List

You delete users from the Email Listeners list when they must no longer receive notifications from Junos Space Network Management Platform.

> **NOTE:** Your role must be assigned the required privileges so that you can delete users from the Email Listeners list.

To delete a user from the Email Listeners list:

1. On the Junos Space Network Management Platform user interface, select **Administration > Email Listeners**.

   The Email Listeners page that appears displays the list of users who receive notifications about the health of the system.

2. Select the e-mail address and click the Delete Email Listener icon (on the right of the page).

   The Confirm dialog box is displayed.

3. You can delete or retain the user from or on the Email Listeners list.

   - To delete the user, click **Yes**.

     The user is deleted from the Email Listeners list.

   - To retain the user, Click **No**.

     The user is retained on the Email Listeners list.

   You are redirected to the Email Listeners page.

RELATED DOCUMENTATION

Adding Users to the Email Listeners List | **1482**

Viewing the Administration Statistics | **1138**

Adding an SMTP Server | **1478**

Replacing a Failed Junos Space Node | **1272**

Modifying Junos Space Network Management Platform Settings | **1346**

CHAPTER 78

Managing Git Repositories

IN THIS CHAPTER

- Git Repositories in Junos Space Overview | 1485
- Managing Git Repositories in Junos Space | 1486
- Viewing Git Repositories in Junos Space | 1490

Git Repositories in Junos Space Overview

Junos Space Network Management Platform Release 15.2R1 enables you to import CLI Configlets and scripts to the Junos Space server from external Git repositories that can be accessed through HTTPS connections. You can add multiple Git repositories from the Administration workspace of Junos Space Platform.

When a Git repository is added from the Administration workspace of Junos Space Platform, a clone of the Git repository is stored on the Junos Space server and this is synchronized with the external Git repository every hour. CLI Configlets and scripts are imported from this clone of the Git repository. Before you import CLI Configlets or scripts, you can synchronize the Git repository clone in Junos Space with the external Git repository to retrieve the latest versions of the files.

Separate Git repositories must be added for importing scripts and CLI Configlets respectively. While multiple Git repositories can be added to Junos Space Platform, only one Git repository of each type can be designated the active repository for importing either scripts or CLI Configlets.

From the Git Repositories inventory page of the Administration workspace, you can view the Git repositories that are configured in Junos Space Platform. You can also add new Git repositories, modify the details of existing Git repositories, delete Git repositories from Junos Space Platform, and designate a Git repository as the active repository. To manage Git repositories in Junos Space Platform, you must be assigned the privileges of a System Administrator.

Release History Table

Release	Description
15.2R1	Junos Space Network Management Platform Release 15.2R1 enables you to import CLI Configlets and scripts to the Junos Space server from external Git repositories that can be accessed through HTTPS connections.

RELATED DOCUMENTATION

- Managing Git Repositories in Junos Space | 1486
- Viewing Git Repositories in Junos Space | 1490
- CLI Configlets Overview | 534
- Scripts Overview | 673

Managing Git Repositories in Junos Space

IN THIS SECTION

- Adding Git Repositories to Junos Space | 1487
- Modifying Git Repositories in Junos Space | 1488
- Deleting Git Repositories from Junos Space | 1488
- Setting the Active Git Repository | 1489
- Testing the Connection to the Git Repository | 1490

In Junos Space Network Management Platform, you can manage Git repository connections from the Git Repositories page of the Administration workspace. External Git repositories are added to Junos Space to enable the import of CLI Configlets and scripts from the repositories to the Junos Space database.

You can perform the following tasks from the **Administration** > **Git Repositories** page of Junos Space Platform:

Adding Git Repositories to Junos Space

You can add multiple Git repositories for importing CLI Configlets and scripts. While adding a Git repository to Junos Space, you can specify whether the Git repository is a configlets repository or a scripts repository.

To add a Git repository to Junos Space:

1. On the Junos Space Platform UI, select **Administration** > **Git Repositories**.

   The Git Repositories page appears, displaying the Git repositories added to Junos Space.

2. Click the **Add Git Repository** icon to add a Git repository.

   The Add Git Repository dialog box is displayed.

3. In the Repository HTTPS URL field, enter the HTTPS URL of the Git repository.

4. (Optional) In the User Name field, enter the username for accessing the Git repository.

   NOTE: If the Git repository does not require user credentials for access, you do not need to enter a username and password. If you choose to enter the username and password, you must enter values in both the fields.

5. (Optional) In the Password field, enter the password of the Git user whose username you entered.

6. (Optional) In the Confirm Password field, reenter the password.

7. From the Type list, select the type of Git repository you are adding.

   You can select either **Configlets** or **Scripts**.

8. (Optional) Select the **Set as active repository** check box to designate the Git repository being added as the active Git repository of that type.

   When you set the active Git repository, the Git repository that was previously the active repository of that type is deactivated.

9. Click **Save** to save the information in Junos Space Platform.

The Git Repository Add Information dialog box appears, displaying the job ID link.

10. Perform one of the following actions:
    - Click the job ID link to view the details of the job on the Job Management page.
    - Click **OK** to return to the Git Repositories page.

      When the job is successfully completed, information about the newly added Git repository is displayed on the Git Repositories page.

Modifying Git Repositories in Junos Space

From the Git Repositories page of the Administration workspace, you can modify the details of the Git repositories that you have added to Junos Space.

To modify the connection details of a Git repository:

1. On the Junos Space Platform UI, select **Administration** > **Git Repositories**.

   The Git Repositories page appears, displaying the Git repositories added to Junos Space.

2. Double-click the row or click the **Edit** icon beside the URL of the Git repository whose details you want to modify.

3. Modify the necessary fields displayed in the inline editor.

   NOTE: The Repository HTTPS URL and Type fields cannot be modified. See "Adding Git Repositories to Junos Space" on page 1487 for more information about modifying the fields.

4. Click **Save** to save your changes.

You are returned to the Git Repositories page where you can see the updated information.

Deleting Git Repositories from Junos Space

You can delete the Git repositories that are added to Junos Space from the Git Repositories page.

To delete the Git repository:

1. On the Junos Space Platform UI, select **Administration** > **Git Repositories**.

   The Git Repositories page appears, displaying the Git repositories added to Junos Space.

2. Select the Git repository you want to delete by clicking the respective row, then click the **Delete** icon at the top of the page.

   A confirmation dialog box appears.

   > **NOTE:** You cannot delete an active Git repository. If you have selected an active Git repository, a warning message is displayed. Click **OK** to return to the Git Repositories page.

3. Click **Yes** to confirm.

You are returned to the Git Repositories page. The deleted Git repository is removed from the page.

Setting the Active Git Repository

In Junos Space Platform, you can add multiple Git repositories, but you can designate only one configlets repository and one scripts repository as the active Git repositories for CLI Configlets and scripts respectively. CLI Configlets and scripts are imported from the active Git repository of that particular type. When you designate a Git repository as an active repository, the previously active repository of that type is no longer active.

To set the active Git repository:

1. On the Junos Space Platform UI, select **Administration** > **Git Repositories**.

   The Git Repositories page appears, displaying the Git repositories added to Junos Space.

2. Select the Git repository you want to mark as active by clicking the respective row.

3. Click the **Set Active Git Repository** icon at the top of the page.

   A confirmation message is displayed.

4. Click Yes to confirm.

   The selected Git repository becomes the new active Git repository of that type. The previously active Git repository of the same type is no longer designated the active Git repository.

The **Active** column on the Git Repositories page displays **Yes** for the active Git repositories.

Testing the Connection to the Git Repository

After you add a Git repository to Junos Space, you can test the connection to make sure that the Git repository is accessible and CLI Configlets or scripts can be imported, depending on the type of Git repository that you added.

To test the connection to the Git repository:

1. On the Junos Space Platform UI, select **Administration** > **Git Repositories**.

   The Git Repositories page appears, displaying the Git repositories added to Junos Space.

2. Select the Git repository for which you want to test the connection by clicking the respective row, then click **Test Connection** at the top right of the page.

   The **Confirm Connection Test** dialog box appears, displaying a message indicating that testing the connection may take several minutes. You are prompted to confirm whether you want to continue.

3. Click **Yes** to confirm.

   The **Status** dialog box appears, displaying the status indicating whether the connection test was successful or failed.

4. Click **OK**.

   You are returned to the Git Repositories page.

RELATED DOCUMENTATION

Git Repositories in Junos Space Overview | 1485

Viewing Git Repositories in Junos Space | 1490

Viewing Git Repositories in Junos Space

In Junos Space Network Management Platform, you can import CLI Configlets and scripts from external Git repositories. Before you import CLI Configlets or scripts from Git repositories, you must add the repositories to Junos Space from the Git Repositories page of the Administration workspace. You can view the details of all the repositories that have been added to Junos Space from the Git Repositories page.

To view Git repositories:

- On the Junos Space Platform UI, select **Administration** > **Git Repositories**.

  The Git Repositories page appears, displaying the Git repositories added to Junos Space.

  Table 188 lists the fields on the Git Repositories page and their descriptions.

  You can use the filter option on the drop-down lists of the **Repository URL** and **Git User Name** column headings to specify the filter criteria. When you apply the filters, the page displays only the Git repositories that match the filter criteria.

Table 188: Git Repositories Page Fields

Field	Description
Repository URL	HTTPS URL of the Git repository
Type	Type of Git repository. Value can be **Configlets** or **Scripts**.
Git User Name	Username for accessing the Git repository
Active	Value can be **Yes** or **No**, indicating whether the Git repository is the active repository or not, respectively

RELATED DOCUMENTATION

Git Repositories in Junos Space Overview | 1485

Managing Git Repositories in Junos Space | 1486

CHAPTER 79

Audit Log Forwarding

IN THIS CHAPTER

- Audit Log Forwarding in Junos Space Overview | 1492
- Viewing Audit Log Forwarding Criterion | 1493
- Adding Audit Log Forwarding Criterion | 1496
- Modifying Audit Log Forwarding Criterion | 1497
- Deleting Audit Log Forwarding Criterion | 1498
- Enabling Audit Log Forwarding Criterion | 1499
- Testing the System Log Server Connection for Audit Log Forwarding | 1500

Audit Log Forwarding in Junos Space Overview

Junos Space Network Management Platform enables you to forward audit logs to a system log server. You can add one or several audit log forwarding criteria to Junos Space Platform to export audit logs from the Junos Space Platform database to a system log server. For example, Criterion1 can be added with HostAddress1 and default port number 514 and default protocol TCP. If Criterion1 is enabled, all audit logs that fulfill Criterion1 are forwarded to HostAddress1.

On the Audit Log Forwarding inventory page of the Administration workspace, you can view the audit log forwarding criteria that are configured in Junos Space Platform. You can also add a new audit log forwarding criterion, enable existing audit log forwarding criteria, modify the details of existing audit log forwarding criteria, and delete audit log forwarding criteria from Junos Space Platform. To manage audit log forwarding in Junos Space Platform, you must be assigned the privileges of a Super Administrator or System Administrator.

Audit logs are forwarded to the system log server at configured time intervals. By default, audit logs are forwarded every sixty minutes. All the audit logs after the previous successful forwarding are exported at the configured time based on an enabled audit log forwarding criterion. You can also enable more than one criteria for audit log forwarding.

The time interval for audit log forwarding can be configured from **Administration** > **Applications**. For more information about configuring the time interval for audit log forwarding, see “Modifying Junos Space Network Management Platform Settings” on page 1346.

The audit logs forwarded to the system log server is in Common Event Format (CEF).

The status of audit log forwarding is displayed by the Audit Logs forwarding failed parameter in the system health report on the Administration page.

When audit log forwarding fails:

- The status of the parameter **Audit log forwarding failed** changes from **No** to **Yes**.
- Configured e-mail listeners in the Email Listeners list receive e-mail alerts (e-mail alerts are also received when the issue is resolved).

For more information about the status of audit log forwarding, see "Viewing the Administration Statistics" on page 1138.

You can perform the following tasks from **Administration** > **Audit Log Forwarding** page of Junos Space Platform:

- Viewing Audit Log Forwarding Criterion on page 1493
- Adding Audit Log Forwarding Criterion on page 1496
- Modifying Audit Log Forwarding Criterion on page 1497
- Deleting Audit Log Forwarding Criterion on page 1498
- Enabling Audit Log Forwarding Criterion on page 1499
- Testing the System Log Server Connection for Audit Log Forwarding on page 1500

Release History Table

Release	Description
16.1R1	Junos Space Network Management Platform enables you to forward audit logs to a system log server.

RELATED DOCUMENTATION

Junos Space Audit Logs Overview | 1115

Viewing Audit Log Forwarding Criterion

In Junos Space Network Management Platform, you can manage audit log forwarding on the Audit Log Forwarding page of the Administration workspace. You can view the details of all configured audit log forwarding criteria on the Audit Log Forwarding page.

You can change the way the audit log forwarding criteria configured in Junos Space Platform are displayed.

To change the way the criteria are displayed:

- On the Junos Space Network Management Platform user interface, select **Administration** > **Audit Log Forwarding**.

  The Audit Log Forwarding page appears, displaying all the configured audit log forwarding criteria in a tabular form.

- Click **Display Quick View** on the Audit Log Forwarding page title bar and click a criterion listed on the page.

  The details of the criterion are displayed on the right side of the Audit Log Forwarding page. You can also disable the Quick View option by clicking on the same button again (**Hide Quick View**).

- Double-click a criterion listed on the Audit Log Forwarding page.

  The details of the selected criterion are displayed in the View Audit Log Forwarding Criterion Details dialog box.

- Select an audit log forwarding criterion from the Audit Log Forwarding page and click the **View Audit Log Forwarding Criterion Details** icon on the title bar.

  The details of the selected criterion are displayed in the View Audit Log Forwarding Criterion Details dialog box.

Table 189 lists the fields on the Audit Log Forwarding page and their descriptions.

You can use the filter option on the **Name**, **Server Address**, **Port**, **Protocol**, **Last Updated User**, **Last Updated Time**, and **Enabled** columns to filter the audit log forwarding criteria. When you apply the filters, the page displays only the audit log forwarding criteria that match the filter criteria.

Table 189: Audit Log Forwarding Page Fields

Field	Description	Location
Name	Name of the audit log forwarding criterion	Audit Log Forwarding Page View Audit Log Forwarding Criterion Details dialog box Quick View

Table 189: Audit Log Forwarding Page Fields *(continued)*

Field	Description	Location
Description	Description of the audit log forwarding criterion	Audit Log Forwarding Page View Audit Log Forwarding Criterion Details dialog box Quick View
Server Address	The address of the system log server to which audit logs are forwarded	Audit Log Forwarding Page View Audit Log Forwarding Criterion Details dialog box Quick View
Port	The port number of the system log server to which audit logs are forwarded The default port number is 514.	Audit Log Forwarding Page View Audit Log Forwarding Criterion Details dialog box Quick View
Protocol	The protocol based on which audit logs are forwarded The options are UDP, TCP, or TLS v1.2. The default protocol used is TCP.	Audit Log Forwarding Page View Audit Log Forwarding Criterion Details dialog box Quick View
Last Updated User	Name of the user who last updated the audit log forwarding criterion	Audit Log Forwarding Page View Audit Log Forwarding Criterion Details dialog box Quick View
Last Updated Time	Date and time when the audit log forwarding criterion was last updated	Audit Log Forwarding Page View Audit Log Forwarding Criterion Details dialog box
Enabled	Status of the audit log forwarding criterion. The value is **Yes** if the criterion is enabled and **No** if it is disabled.	Audit Log Forwarding Page View Audit Log Forwarding Criterion Details dialog box Quick View

Table 189: Audit Log Forwarding Page Fields *(continued)*

Field	Description	Location
Filter Criteria	Parameters included in the criterion to enable filtering of the audit logs sent to the system log server.	View Audit Log Forwarding Criterion Details dialog box

RELATED DOCUMENTATION

- Audit Log Forwarding in Junos Space Overview | **1492**
- Adding Audit Log Forwarding Criterion | **1496**
- Modifying Audit Log Forwarding Criterion | **1497**
- Deleting Audit Log Forwarding Criterion | **1498**
- Enabling Audit Log Forwarding Criterion | **1499**
- Testing the System Log Server Connection for Audit Log Forwarding | **1500**

Adding Audit Log Forwarding Criterion

You can add an audit log forwarding criterion for exporting audit logs to a system log server. To add a criterion, you need Super Administrator or System Administrator privileges.

To add an audit log forwarding criterion:

1. On the Junos Space Network Management Platform user interface, select **Administration** > **Audit Log Forwarding**.

   The Audit Log Forwarding page appears displaying the list of configured audit log forwarding criteria.

2. On the menu bar, click **Create Audit Log Forwarding Criterion** (the plus icon).

   The Add Audit Log Forwarding Criterion page appears.

3. Enter the following details.
   - **Name**: Enter the name for the audit log forwarding criterion.
   - (Optional) **Description**: Enter a short description for the criterion.
   - **Syslog Host Address**: Enter the host address of the system log server. It must either be a fully qualified domain name (FQDN) or the IP address of the system log server.

- **Port Number**: Enter the port number of the system log server. The default port number is 514.
- **Protocol**: Select the protocol from the given list. You can select UDP, TCP, or TLS v1.2. The default protocol used is TCP.
- (Optional) To enable filtering of the audit logs to be sent to the system log server, select the **Include Filters** check box. Selecting this check box enables you to filter out audit logs based on the different parameters displayed on the Audit Log page under the Audit Logs workspace.

  NOTE: If **Include Filters** is not selected, all the audit logs generated in Junos Space are forwarded to the configured system log server.

- (Optional) To enable the criterion, select the **Enable this forwarding criterion** check box.

4. Click **Save** to save the audit log forwarding criterion.

   The new criterion is created and the Add Audit Log Forwarding Criterion dialog is displayed with the corresponding Job ID.

   (Optional) On clicking the Job ID, you are redirected to the **Jobs > Job Management** page with a filtered view of the Job corresponding to addition of the new audit log forwarding criterion.

RELATED DOCUMENTATION

Audit Log Forwarding in Junos Space Overview | 1492

Viewing Audit Log Forwarding Criterion | 1493

Modifying Audit Log Forwarding Criterion | 1497

Deleting Audit Log Forwarding Criterion | 1498

Enabling Audit Log Forwarding Criterion | 1499

Testing the System Log Server Connection for Audit Log Forwarding | 1500

Modifying Audit Log Forwarding Criterion

In Junos Space Network Management Platform, you can forward audit logs to a system log server. As a Super Administrator or System Administrator, you can modify an existing audit log forwarding criterion.

To modify an existing criterion:

1. On the Junos Space Network Management Platform user interface, select **Administration** > **Audit Log Forwarding**.

   The Audit Log Forwarding page appears.

2. Select the audit log forwarding criterion to be modified.

3. On the menu bar, click **Modify Audit Log Forwarding Criterion** (the pencil icon).

   The Modify Audit Log Forward Criterion page appears.

4. Modify the required fields.

   You can modify Description, Syslog Host Address, Port Number, and Protocol. You can also check or uncheck the **Include Filters** check box. You cannot modify the name of the audit log forwarding criterion.

5. Click **Save** to save the modification.

   The modification is saved and the Modify Audit Log Forwarding Criterion dialog is displayed with the corresponding Job ID.

   (Optional) On clicking the Job ID, you are redirected to the **Jobs > Job Management** page with a filtered view of the Job corresponding to modification of the audit log forwarding criterion.

RELATED DOCUMENTATION

- Audit Log Forwarding in Junos Space Overview | **1492**
- Viewing Audit Log Forwarding Criterion | **1493**
- Adding Audit Log Forwarding Criterion | **1496**
- Deleting Audit Log Forwarding Criterion | **1498**
- Enabling Audit Log Forwarding Criterion | **1499**
- Testing the System Log Server Connection for Audit Log Forwarding | **1500**

Deleting Audit Log Forwarding Criterion

You can delete one or several audit log forwarding criteria configured in Junos space Network Management Platform. You must have Super Administrator or System Administrator privileges to delete criteria.

To delete audit log forwarding criteria:

1. On the Junos Space Network Management Platform user interface, select **Administration** > **Audit Log Forwarding**.

   The Audit Log Forwarding page appears.

2. Select the criteria to be deleted from the list of existing criteria on the Audit Log Forwarding page.

3. On the menu bar, click **Delete Audit Log Forwarding Criteria** (the minus icon).

   The Delete Audit Log Forwarding Criteria dialog box is displayed.

4. Click **Delete** to delete the criterion or **Cancel** to cancel the action.

   The Audit Log Forwarding page displays the current list of criteria configured on Junos Space Platform.

RELATED DOCUMENTATION

- Audit Log Forwarding in Junos Space Overview | **1492**
- Viewing Audit Log Forwarding Criterion | **1493**
- Adding Audit Log Forwarding Criterion | **1496**
- Modifying Audit Log Forwarding Criterion | **1497**
- Enabling Audit Log Forwarding Criterion | **1499**
- Testing the System Log Server Connection for Audit Log Forwarding | **1500**

Enabling Audit Log Forwarding Criterion

Use the Audit Log Forwarding page under the Administration workspace to enable forwarding of audit logs to a system log server based on one or several criteria configured in Junos Space Network Management Platform. The criteria can be enabled by a user with Super Administrator or System Administrator privileges.

To enable an audit log forwarding criterion:

1. On the Junos Space Network Management Platform user interface, select **Administration** > **Audit Log Forwarding**.

   The Audit Log Forwarding page appears.

2. Select the criterion to be enabled from the list of existing criteria on the Audit Log Forwarding page.

3. On the menu bar, click **Enable Audit Log Forwarding Criterion**.

   The Enable Audit Log Forwarding Criterion dialog box is displayed.

4. Click **Confirm** to enable the criterion or **Cancel** to cancel the action.

   If you click Confirm, the Audit Log Forwarding page is displayed with the current list of configured criteria, and the **Enabled** column of the enabled criteria shows the status **Yes**.

> **NOTE:** On the menu bar, **Enable Audit Log Forwarding Criterion** changes to disabled state when an enabled criterion is selected.

RELATED DOCUMENTATION

- Audit Log Forwarding in Junos Space Overview | 1492
- Viewing Audit Log Forwarding Criterion | 1493
- Adding Audit Log Forwarding Criterion | 1496
- Modifying Audit Log Forwarding Criterion | 1497
- Deleting Audit Log Forwarding Criterion | 1498
- Testing the System Log Server Connection for Audit Log Forwarding | 1500

Testing the System Log Server Connection for Audit Log Forwarding

After you add an audit log forwarding criterion to Junos Space Network Management Platform, you can test to make sure that the system log server is active and audit logs can be forwarded to it based on the enabled criteria.

To test the connection to the system log server:

1. On the Junos Space Network Management Platform user interface, select **Administration** > **Audit Log Forwarding**.

   The Audit Log Forwarding page appears.

2. Select the criterion to be tested from the list of existing criteria on Audit Log Forwarding page.

3. On the menu bar, click **Test Syslog Server Connection**.

The Test Syslog Server Connection dialog box is displayed.

4. Click **Yes** to test the connection or **Cancel** to cancel the action.

   If you click **Yes**, the Syslog Connection Status dialog box is displayed with the status of the connection for the selected criterion as active/inactive.

RELATED DOCUMENTATION

- Audit Log Forwarding in Junos Space Overview | **1492**
- Viewing Audit Log Forwarding Criterion | **1493**
- Adding Audit Log Forwarding Criterion | **1496**
- Modifying Audit Log Forwarding Criterion | **1497**
- Deleting Audit Log Forwarding Criterion | **1498**
- Enabling Audit Log Forwarding Criterion | **1499**

CHAPTER 80

Configuring a Proxy Server

IN THIS CHAPTER

- Configuring Proxy Server Settings | 1502

Configuring Proxy Server Settings

From the Administration workspace, you can configure a proxy server that Junos Space Network Management Platform and its installed applications can use. For example, when you initiate an action to download the DMI schemas from the Subversion repository of Juniper Networks, Junos Space Platform accesses the Subversion repository through the proxy server, if the proxy server is configured.

You can configure a proxy server in Junos Space Platform if you are a user who is assigned the privileges of a Super Administrator or System Administrator. If you are a User Administrator creating a custom role, you can assign the privileges of a Super Administrator or System Administrator to the new role so that when you assign this role to a user, the user has the necessary permissions to configure a proxy server.

To configure a proxy server:

1. On the Junos Space Platform user interface, select **Administration** > **Proxy Server**.

   You are taken to the Proxy Server page. If an existing proxy server is configured, the settings are displayed.

2. Click the pencil icon (**Add/Edit Proxy server**) to add a proxy server or edit an existing proxy server.

   The fields on the Proxy Server page can now be edited.

3. In the **Proxy Address** text box, enter the IP address of the proxy server.

NOTE:

- Depending on whether the Junos Space fabric is configured with only IPv4 addresses or both IPv4 and IPv6 addresses, Junos Space Platform allows you to enter an IPv4 address or either an IPv4 or IPv6 address respectively for the proxy server.
- The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to http://www.iana.org/assignments/ipv4-address-space for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space for the list of restricted IPv6 addresses.

4. In the **Port** text box, enter the port number of the proxy server.

   You must enter a port number that must be in the range 0 through 65,535.

5. (Optional) In the **User Name** text box, enter the username that you want to use for authentication.

   The maximum number of characters allowed is 255; other restrictions may be imposed by the proxy server depending on its configuration.

6. (Optional) Enter the authentication password in the **Password** text box.

   The maximum number of characters allowed is 255; other restrictions may be imposed by the proxy server depending on its configuration.

7. Do one of the following:

   - Click **Save** to save the proxy server configuration.

     The proxy server settings that you entered are saved and the fields on the page are no longer editable.

   - Click **Cancel** to cancel the proxy server configuration.

     The proxy server settings that you entered are discarded and the fields on the page are no longer editable.

   NOTE: Optionally, you can click **Clear** to clear the proxy server settings that you entered, and reenter the proxy server settings.

8. To enable the proxy server configuration, select the **Enable Proxy Server** check box.

NOTE: You must enable the proxy server configuration for Junos Space Platform to use the configured proxy server.

Junos Space Platform and applications installed on Junos Space Platform can use the configured proxy server.

RELATED DOCUMENTATION

Junos Space Administrators Overview | 1136

CHAPTER 81

Managing Tags

IN THIS CHAPTER

- Tags Overview | **1506**
- Creating a Tag | **1507**
- Managing Tags | **1512**
- Managing Hierarchical Tags | **1513**
- Sharing a Tag | **1521**
- Renaming Tags | **1522**
- Deleting Tags | **1523**
- Tagging an Object | **1526**
- Untagging Objects | **1527**
- Filtering the Inventory by Using Tags | **1528**
- Viewing Tagged Objects | **1529**
- Viewing Tags for a Managed Object | **1532**
- Exporting Tags from Junos Space Network Management Platform | **1533**

Tags Overview

You can create user-defined tags on an application workspace inventory page to easily categorize and organize managed objects. Subsequently, you can view and use these tags to easily search for multiple objects to view the status or perform a bulk action on them without having to select each object individually.

Tags are classified into two categories: private tags and public tags. Private tags are those that are created by you and can be used only by you because they are not visible to others. Public tags are those that are available to all users for tagging objects that are accessible to them. You need the Tag Administrator role privileges to create, modify, or delete a public tag, manage hierarchical tags, as well as convert a private tag to a public tag. However, any Junos Space user can:

- Create, modify, and delete private tags
- View public and private tags
- Tag and untag objects by using public and private tags
- Export public and private tags

> **NOTE:** You cannot view or access private tags created by other users. However, if you are a user with the Tag Administrator role, you can view and access private tags of other users.

Tag names should not start with a space; contain a comma, double quotation marks, or parentheses; and exceed 255 characters. Also, you cannot name a tag “Untagged” because it is a reserved term.

To use tags:

1. Create a private or public (shared tag) by using the **Administration** > **Tags** > **Create Tag** user interface (see “Creating a Tag” on page 1507), or from a Device Management or Job Management inventory landing page (see “Managing Hierarchical Tags” on page 1513).

2. Tag an object on an inventory page. For example, you can tag an object on the Device Management inventory page. After you tag an object, you can view or untag existing tags. See “Tagging an Object” on page 1526 and “Untagging Objects” on page 1527.

3. (Optional) Create hierarchical tags and manage them on the Tag Hierarchy pane in the Tag view on an inventory landing page for taggable objects (such as devices or jobs). See “Managing Hierarchical Tags” on page 1513.

4. Manage tags using the **Administration** > **Tags** inventory page, or a Device Management or Job Management inventory landing page. You can view, share, rename, or delete tags, as well as view the list of objects assigned to a tag from this page. See “Viewing Tags for a Managed Object” on page 1532,

"Sharing a Tag" on page 1521, "Renaming Tags" on page 1522, "Deleting Tags" on page 1523, and "Viewing Tagged Objects" on page 1529.

My Favorite Private Tag

When you mark an object as favorite for the first time, a private tag named My Favorite is created automatically. After the My Favorite tag is created, all objects marked using the Mark as Favorite workflow are assigned the My Favorite tag. You can access this tag from any of the inventory landing pages that allow you to select objects by tags. You cannot modify the My Favorite tag to a public tag. Currently, CLI Configlets, scripts, or scripts in a script bundle can be marked as favorites. When you unmark an object as favorite by using the Unmark as Favorite workflow, the object is untagged from the My Favorite tag.

Device Tags

Device tags are tags that are applicable only to devices and associate a tag with the IP address or hostname of a device managed by Junos Space Platform. Device tags are uploaded in the CSV format. You can associate the IP address or hostname with a custom tag and categorize the tag as a public or private tag. These tags can be used to filter devices when deploying a device template, upgrading a device image, staging scripts, or applying CLI Configlets to devices through workflows that enable filtering by tags.

For more information about creating and uploading device tags by using a CSV file, see "Uploading Device Tags by Using a CSV File" on page 211.

RELATED DOCUMENTATION

- Tagging an Object | 1526
- Untagging Objects | 1527
- Filtering the Inventory by Using Tags | 1528
- Viewing Tagged Objects | 1529
- Managing Hierarchical Tags | 1513

Creating a Tag

You create tags to label and categorize Junos Space Network Management Platform objects so that you can filter, monitor, or perform batch actions on the tagged devices without having to select each object individually. All users can create their own private tags from the **Administration > Tags** inventory landing page. Users assigned the Tag Administrator role can create public tags.

You can create tags from the Administration workspace as well as from the Device Management or Job Management inventory landing page. By default, the tags that any user creates are private tags, which means that these tags are visible only to the user who creates them. No other user can access the private tags created by other users. However, if you are a user with the Tag Administrator role, you can make these tags public, thereby allowing all users to associate objects with these tags.

To create a tag from the Administration workspace:

1. On the Junos Space Network Management Platform user interface, select **Administration** > **Tags**.

   The Tags page appears.

2. On the toolbar, click the **Create Tag** icon.

   The **Create Tag** dialog box appears.

3. If necessary, select the **Share this Tag** check box.

   When you share a tag, all users can use that tag. Only users with the Tag Administrator role can publish tags to the public domain. For users without this role, the **Share this Tag** check box is disabled (grayed out).

4. In the **Tag Name** field, type a tag name.

   You can enter an alphanumeric string for the tag name. The tag name can also contain underscores, hyphens, and spaces. However, a tag name should not:

   - Exceed 255 characters
   - Start with a space
   - Contain special characters, such as commas, double quotation marks, or parentheses.

   NOTE: “Untagged” is a reserved term and hence you cannot create a tag with this name.

5. Click **Create**.

   The Create Tag dialog box appears, displaying that the tag is successfully created.

6. Click **OK** on the Create Tag dialog box.

   The newly added tag appears on the Tags page. If the tag is shared, it is public; if not, it is private. The **Access Type** column displays whether the tag is public or private.

In addition to creating tags from the Administration workspace, you can create tags from the following inventory landing pages as well:

- Device Management
- Job Management

For example, to create a tag from the Device Management inventory landing page:

1. On the Junos Space Network Management Platform user interface, click **Devices** > **Device Management**.

   The Device Management page appears.

2. If the tags are not displayed, click the **Display Tag View** icon on the toolbar located at the top of this page.

   On the left side of the page, tags that are relevant to the page and the domain to which you are logged in are displayed.

   > **NOTE:** Tags from domains other than the domain to which the user is logged in are not displayed.

   In Tags View, the tags are categorized as follows:

   - **Public**—Lists public tags. Public tags are tags that are visible and available to all users and can be used by any user to tag an object in Junos Space.

     You can perform the following actions on public tags:

     - Mouse over a tag to view the number of objects that are associated with the specific tag.
     - Click a tag to view the devices associated with the selected tag. The number displayed adjacent to the tag shows the number of devices associated with the specific tag. For example, if you have assigned this tag to two devices, then the number displayed is 2. However, this rule has the following exceptions:
       - For hierarchical tags, the count on the parent tag does not include the number of objects associated with its child tags. For example, if a child tag is associated with 10 objects and its parent tag is associated with five objects, then the count displayed for the parent tag is 5 and not 15.
       - You used the same tag on objects other than devices. For example, if you assigned TagC to UserA and DeviceB, then on the Device Management page, the count shown for TagC is 1. However, when you mouse over TagC, the tooltip displays a count of 2 (which includes the object type as well—in this example, the object types that are displayed are **User** and **Device**).

   - **Private**—Lists private tags. Private tags are tags that you created and hence are visible only to you. No other user has access to these tags.

Click a tag to view the devices associated with the selected tag. The number displayed adjacent to the tag shows the number of devices that are associated with the specific tag. For example, if you assigned this tag to two devices, then the number displayed is 2.

- **Untagged**—Displays the number of devices that are not tagged

3. (Optional) To view all tags (that is, tags that are relevant and irrelevant to the inventory landing page to which you are currently logged in), select **Show All Tags** on the **Tags** list at the top of the Device Management inventory landing page.

   By default, **Show Relevant Tags** is selected and only the tags that are relevant to the current inventory landing page are displayed.

4. To add a tag:

   a. Click the **Add Tag** icon.

   > **NOTE:** If you use the shortcut menu instead of the Add Tag icon, the new tag that is added is of the same type as that of the parent. For example, right-click **Private** and select **Add Tag** to create a private tag.

   b. In the **Tag Name** field, type a tag name.

      A tag name can be an alphanumeric string that contains underscores, hyphens, and spaces. However, note that a tag name should not:

      - Exceed 255 characters
      - Start with a space
      - Contain special characters, such as commas, double quotation marks, or parentheses.

      > **NOTE:** "Untagged" is a reserved term and hence you cannot create a tag with this name.

   c. If necessary, select the **Make Public** check box to create a public tag. If left unselected, a private tag is created.

      When you make a tag public, all users can use that tag. Only the Tag Administrator can publish tags to the public domain.

      > **NOTE:** This check box is disabled if you chose to create a tag by using the shortcut menu. The new tag that is added is of the same type as that of the parent.

d. (Optional) In the **Description** field, add a description of the tag.

e. Click **Add Tag**.

   The tag is added to the relevant tag category and assigned to the domain to which you are currently logged in. For example, if you created a public tag, the newly added tag is placed in the **Public** category. The count is set to zero (0) because you have not assigned this tag to any object.

> **NOTE:** You cannot add any tags to the **Untagged** category.

When you add a tag, an audit log entry is automatically generated.

RELATED DOCUMENTATION

- Tags Overview | **1506**
- Managing Tags | **1512**
- Sharing a Tag | **1521**
- Renaming Tags | **1522**
- Deleting Tags | **1523**

Managing Tags

You can use tags to label and categorize objects in your network, such as subnets, devices, services, users, customers, and so forth so you can filter, monitor, or perform batch actions on them without having to select each object separately. You can also use tags to select devices. The inventory page allows you to manage and manipulate personal tags that you created. You must have the Super Administrator, System Administrator, or Tag Administrator role to manage tags.

The Tags page is empty for a new Junos Space installation until you create public and private tags. However, if you have upgraded from a previous release, then public and private tags from the preupgraded setup are listed on the Tags page. Tags are visible only to you unless the Tag Administrator shares them and makes them public to all users. Tags created by other users are private and visible only to them unless the Tag Administrator shares them and makes them public to all users.

You can manage all tags applied to inventory objects from the **Administration** > **Tags** inventory page. You can share, rename, or delete tags. You can view the list of objects assigned to a tag from the Tags page.

Viewing Tags

To view tags on the inventory page:

- All tags appear on the inventory page in tabular view and are listed alphabetically by tag name.

  You can filter inventory objects by tag name (see "Filtering the Inventory by Using Tags" on page 1528).

Viewing Tag Information

Tag data includes tag name, tag owner, access type, and number of objects tagged by a particular tag. See Table 190.

Table 190: Tag Information

Tag Data	Description
Name	Unique tag name. Tag names cannot start with a space or be longer than 256 characters.
Owner	Owner of a private tag. Public tags do not have a specific owner and hence this column is empty for public tags. A user with the Super Administrator role can view private tags of all users, whereas a user without this role can view only the private tags created by that user.
Access Type	Tags can be public (shared) or private (visible only to the creator).
Tagged Object Count	Number of objects tagged in all workspace inventory pages by the tag. You can click the link to view the objects that are assigned to a specific tag.

You can sort and hide columns. You can also filter data on the Name, Owner, and Access Type columns. For more information about manipulating tables in tabular view, see "Junos Space User Interface Overview" on page 89 in the *Junos Space User Interface Guide*.

Performing Actions on Tags

To perform an action on one or more tags:

1. Select one or more tags in the table.

   Click a tag to select it. If you select one tag, you can perform all tag-management actions. If you select two or more tags, you can only delete the tags.

2. Select a command from the Actions menu or the shortcut menu.

   You can share (see "Sharing a Tag" on page 1521), rename (see "Renaming Tags" on page 1522), delete (see "Deleting Tags" on page 1523, or deselect all selected tags. You can also view the objects that are assigned the selected tag ("Viewing Tagged Objects" on page 1529).

RELATED DOCUMENTATION

- Tags Overview | **1506**
- Tagging an Object | **1526**
- Viewing Tags for a Managed Object | **1532**
- Untagging Objects | **1527**
- Creating a Tag | **1507**

Managing Hierarchical Tags

Hierarchical tags consist of multiple levels of tags within a single tag. You can use hierarchical tags to classify objects managed by Junos Space Network Management Platform into categories and subcategories. Hierarchical tagging uses other tags to classify a tag. The hierarchy allows you to drill down to the specific objects in Junos Space Network Management Platform very easily.

A hierarchical tag contains parent and child tags. For example, if you have an existing tag named West Coast and you create another tag within this tag named California, then the West Coast tag is the parent tag and the California tag is the child tag.

NOTE: Only public tags can be hierarchical. That is, you can create a public tag within another public tag.

You can view, create, update, and delete hierarchical tags on the **Devices** > **Device Management** inventory page and **Jobs** > **Job Management** inventory page. For more information about creating, modifying, and deleting tags, see "Using the Shortcut Menu" on page 1516. This topic contains information about working with tags on the Device Management page. You can extend this information to the Job Management page.

The **Devices** > **Device Management** inventory page displays all devices on the network that are accessible to you and that are managed by Junos Space Network Management Platform. To filter devices on the basis of tags:

1. Click the **Display Tag View** icon on the toolbar.

   The Tag Hierarchy pane appears, which displays a tree view of all tags (public and private tags) that are relevant to the inventory landing page that you are currently on.

   You can view, create, update, and delete tags on this pane.

2. Mouse over a tag to view the number of objects assigned to a public or private tag.

   The Tag Hierarchy pane also displays the **Untagged** category, which lists the number of devices that are not tagged.

3. Select a public or private tag on the tag hierarchy tree to filter devices that are assigned the selected tag. The devices tagged assigned with this specific tag appear in a tabular view (also called Tabular View Pane).

   If you click **Untagged**, the devices that are untagged are displayed.

- Using the Tag Hierarchy Pane | **1514**
- Using the Tabular View Pane | **1520**

Using the Tag Hierarchy Pane

IN THIS SECTION

- Using the Tag Action Bar | **1515**
- Using the Shortcut Menu | **1516**
- Using Drag-and-Drop | **1518**
- Using the Quick Info Tool Tip | **1519**

- Browsing Tagged Objects | **1519**
- Viewing All Tags | **1519**
- Adding a Child Tag | **1520**
- Deleting a Tag | **1520**
- Using Notification | **1520**

The Tag Hierarchy pane displays all tags organized hierarchically in a tree view. You can view, create, update, and delete tags in this pane.

To display the Tag Hierarchy pane, click the **Display Tag View** icon on the **Devices > Devices Management** inventory page.

Using the Tag Action Bar

You can use the Tag Action bar to add a tag or delete an existing tag in the tag hierarchy tree. The Tag Action bar has two buttons—the plus [+] button and the minus [–] button. You can click the plus [+] button to add a child tag and the minus [–] button to delete a tag in the tag hierarchy tree.

> **NOTE:** Only public tags can be hierarchical. That is, you can create a public tag within another public tag.

To add a public or private tag:

1. Select the **Public** or **Private** category depending on the type of tag that you want to add.

2. Click the **Add Tag** (plus [**+**] button) on the Tag Action bar. This option is disabled if you do not have the necessary permissions.

   The Create Tag dialog box appears.

3. Type a new tag name in the **Tag Name** field.

   You can enter an alphanumeric string for the tag name. The tag name can also contain underscores, hyphens, and spaces. However, a tag name should not:

   - Exceed 255 characters
   - Start with a space
   - Contain special characters, such as commas, double quotation marks, and parentheses

> **NOTE:** "Untagged" is a reserved term and hence you cannot create a tag with this name.

4. Select the **Make Public** check box.

   If you do not select this check box, then a private tag is created.

5. Click the **Add Tag** button.

   A new tag is added to the tag hierarchy.

To delete a tag:

1. Select the tag you want to delete from the tag hierarchy tree.

2. Click the **Delete Tag** (minus [–] button) on the Tag Action bar. This option is disabled if you do not have the necessary permissions.

   A confirmation dialog box appears.

> **NOTE:** If you are deleting a child tag and you want to remove the child tag completely from Junos Space Network Management Platform, select the **Also delete <*tag-name*> tags** check box on the confirmation dialog box. If this check box is not selected and if the selected tag appears in multiple locations, then it is deleted from the current location only.

> **CAUTION:** If you have assigned this tag to any object, then the object-tag association is lost when you click **Yes** on the confirmation dialog box.

3. Click **Yes** to delete the tag.

> **NOTE:** The tag is deleted and any object-tag association is lost. However, you can click **No** on the confirmation dialog box to prevent this and the tag is not deleted.

Using the Shortcut Menu

When you right-click a tag in the tag hierarchy tree, a shortcut menu appears.

This menu displays the **Add Tag**, **Remove Tag**, and **Modify Tag** options. Use the **Add Tag** option to add a new child tag in case of a public tag or to add a new private tag. Use **Modify Tag** and **Remove Tag** options to modify and delete a tag, respectively.

> **NOTE:** Only public tags can be hierarchical. That is, you can create a public tag within another public tag.

To add a child tag by using the shortcut menu:

1. Right-click a public tag in the tag hierarchy tree for which you want to add a child tag.

   The shortcut menu appears.

2. Click the **Add Tag** option on the shortcut menu. This option is disabled if you do not have the necessary permissions.

   The Create Tag dialog box appears.

3. Type a new tag name in the field.

   You can enter an alphanumeric string for the tag name. The tag name can also contain underscores, hyphens, and spaces. However, a tag name should not:

   - Exceed 255 characters
   - Start with a space
   - Contain special characters, such as commas, double quotation marks, and parentheses

   > **NOTE:** “Untagged” is a reserved term and hence you cannot create a tag with this name.

4. Click the **Add Tag** button.

   A new child tag is added to the tag hierarchy.

To modify a tag by using the shortcut menu:

1. Select the tag you want to modify from the tag hierarchy tree.

2. Click the **Modify Tag** option on the shortcut menu. This option is disabled if you do not have the necessary permissions.

   The Edit Tag Name or Description dialog box appears.

3. Edit the tag name or the description, as needed.

4. Click **Modify Tag** to modify the tag.

> **NOTE:** If you have assigned this tag to any object, then those objects are associated with the modified tag.

To delete a tag by using the shortcut menu:

1. Select the tag you want to delete in the tag hierarchy tree.

2. Click the **Delete Tag** option on the shortcut menu. This option is disabled if you do not have the necessary permissions.

   A confirmation dialog box appears.

> **NOTE:** If you are deleting a child tag and you want to remove the child tag completely from Junos Space Network Management Platform, select the **Also delete *<tag-name>* tags** check box on the confirmation dialog box. If this check box is not selected and if the selected tag appears in multiple locations, then it is deleted from the current location only.

> **CAUTION:** If you have assigned this tag to any object, then the object-tag association is lost when you click **Yes** on the confirmation dialog box.

3. Click **Yes** to delete the tag.

> **NOTE:** The tag is deleted and any object-tag association is lost. However, you can click **No** on the confirmation dialog box to prevent this and the tag is not deleted.

Using Drag-and-Drop

You can drag a public tag from one location and drop it in another location to manipulate the tag hierarchy. When you drag and drop a tag from one location to another, the corresponding tagged objects are not affected. For example, if the tag is associated with five devices, then it remains associated with the same five devices after you drag and drop the tag from one location to another.

When you try to drag a public tag from one location to another, you can either move the tag from the current location to another location or copy the tag. The copy operation is used to make an identical copy of the tag in the new location, whereas the move operation is used to move the tag from the current location to a new location.

> **NOTE:** You can move tags only within the public tags hierarchy. If you do not have permissions to create or delete tags, you cannot move tags.

Using the Quick Info Tool Tip

The Quick Info tool tip provides quick and immediate statistics about a tag. You can place the cursor over a tag name or a tag icon in the tag hierarchy tree to see a quick summary of its tagged objects.

To view the tool tip for a tag:

1. Select a particular tag in the tag hierarchy tree.

2. Place the cursor over the tag icon or the tag name.

   Brief statistics about the tagged objects appear.

Browsing Tagged Objects

When you browse the tag hierarchy tree and select a tag, the corresponding tagged objects appear in the Tabular View pane. When you select the root node in the tag hierarchy tree, all tagged objects appear in the Tabular View pane without any filtering.

You can click the [X] icon in the Tabular View pane to clear tag filtering. When you clear tag filtering, the root node in the tag hierarchy tree is automatically selected and all tagged objects appear in the Tabular View pane.

Viewing All Tags

By default, the tag hierarchy tree displays tags relevant to the **Device Management** inventory page only. In this mode, only those tags appear that are either empty or a tag that has at least one object on the inventory page. This is because **Show Relevant Tags** is selected by default on the **Tags** list located at the top of the Tag Hierarchy pane.

To view all public tags:

1. Navigate to the Tags toolbar at the top of the Tag Hierarchy pane.

2. Select the **Show All Tags** option from the Tags list.

   All public tags appear in the Tabular View pane on the right.

Adding a Child Tag

You can use either the Tag Action bar or the shortcut menu to add a child tag to the tag hierarchy tree. To add a child tag by using the Tag Action bar, see "Using the Tag Action Bar" on page 1515. To add a child tag by using the shortcut menu, see "Using the Shortcut Menu" on page 1516.

Deleting a Tag

You can use either the Tag Action bar or the shortcut menu to delete a tag from the tag hierarchy tree. To delete a tag by using the Tag Action bar, see "Using the Tag Action Bar" on page 1515. To delete a tag by using the shortcut menu, see "Using the Shortcut Menu" on page 1516.

Using Notification

When multiple Junos Space Network Management Platform users view the same tag view on the **Device Management** inventory page, any change a user makes is immediately updated in the other tag views. Changes include creating, updating, and deleting tags in the Tag View pane, and tagging objects in the Tabular View pane.

Using the Tabular View Pane

The Tabular View pane displays all managed objects as rows in a table. When you select a particular tag in the tag hierarchy tree, its corresponding tagged objects are displayed in this pane.

In this view, you can tag objects and also search for objects tagged with a particular tag.

Tagging an object by using a hierarchical tag in the Tabular View pane is similar to tagging an object using a nonhierarchical tag on any application workspace manage inventory page. For information about how to tag an object, see "Tagging an Object" on page 1526.

To search for specific tagged objects:

1. Navigate to the Device Management page.

2. Select a tag in the search box.

   The tag hierarchy tree navigates to the selected tag, and the Tabular View pane displays the objects that are tagged with that particular tag only.

RELATED DOCUMENTATION

Tags Overview | **1506**

Sharing a Tag

User-defined tags are always created as private tags initially. If your tag has public value, you can share it to make it public for all users to tag objects on a workspace inventory page. To share a tag, you must have Tag Administrator privileges.

To share a tag.

1. On the Junos Space Network Management Platform user interface, select **Administration** > **Tags**.

   The **Tags** inventory page appears.

2. Select one or more private tags on the inventory page. The **private** keyword in the **Access Type** column on the Tags page indicates private tags.

3. Select **Make Tag Public** from the Actions menu or the shortcut menu.

   The **Share Tag** status box indicates whether you have shared the tag successfully.

   You can also share a tag when you add a new tag. (see "Creating a Tag" on page 1507).

4. Click **OK** on the Share Tag status box.

   The **Access Type** of the tag changes on the inventory table from **private** to **public**.

   > **NOTE:** You cannot revert a public tag to a private tag.

When you share a tag, an audit log entry is automatically generated.

RELATED DOCUMENTATION

- Tags Overview | **1506**
- Managing Tags | **1512**
- Renaming Tags | **1522**
- Deleting Tags | **1523**
- Creating a Tag | **1507**

Renaming Tags

The Modify Tag command enables you to reorganize or recatagorize managed objects according to your changing needs.

To rename a tag:

1. On the Junos Space Network Management user interface, select **Administration** > **Tags**.

   The Tags inventory page appears.

2. Select the tag that you want to rename.

3. Select **Modify Tag** from the shortcut menu.

   The **Modify Tag** dialog box appears.

4. Type a tag name in the **New Name** field.

   A tag name should not start with a space, cannot contain a comma, double quotation marks, and parentheses, or exceed 255 characters. Also, “Untagged” is a reserved term and hence you cannot have a tag with this name.

5. Click **Modify**.

   The old tag is renamed and saved in the database. You see the renamed tag on the inventory page. The objects that were associated with the old tag are now associated with the modified tag.

You can rename a tag not only from the Tags workspace but also from other workspaces such as the Device Management inventory landing page or the Job Management inventory landing page.

To rename a tag from the Device Management inventory landing page:

1. On the Junos Space Network Management Platform user interface, select **Devices** > **Device Management**.

   The Device Management page appears.

2. If tags are not displayed, click the **Display Tag View** icon on the toolbar.

3. Select a tag and click **Modify Tag** from the shortcut menu.

4. Type a tag name in the **Tag Name** field.

A tag name should not start with a space, cannot contain a comma, double quotation marks, and parentheses, or exceed 255 characters. Also, “Untagged” is a reserved term and hence you cannot have a tag with this name.

5. Modify the description in the **Description** field.

6. Click **Modify**.

   The old tag is renamed and saved in the database. You see the renamed tag on the inventory page. The objects that were associated with the old tag are now associated with the modified tag.

When you modify a tag, an audit log entry is automatically generated.

RELATED DOCUMENTATION

- Tags Overview | **1506**
- Managing Tags | **1512**
- Sharing a Tag | **1521**
- Deleting Tags | **1523**
- Creating a Tag | **1507**
- Filtering the Inventory by Using Tags | **1528**.

Deleting Tags

Use Delete Tags to remove tags that you no longer need.

NOTE:

- You can delete a public tag only if you have sufficient permissions. Contact your system administrator if this need arises.
- Private tags created by other users are not visible to you and hence you cannot delete them. Even a user with the Tag Administrator role is not permitted to delete private tags of other users.

  You can delete your private tags not only from the Tags inventory page but also from any inventory page where deletion of private tags is permitted. Select **Delete Private Tags** from the Actions menu on the respective inventory landing page.
- You cannot delete the top-level **Public**, **Private**, or **Untagged** categories. You can delete the tags only within the **Public** and **Private** categories.

To delete a public or a private tag from the Tags workspace:

1. On the Junos Space Network Management Platform user interface, select **Administration** > **Tags**.

   The **Tags** page appears.

2. Select one or more tags that you want to delete.

3. Select **Delete Tags** from the shortcut menu.

   This option is disabled if you do not have sufficient permissions to delete the selected tags. This situation may arise when you are trying to delete a public tag for which you do not have the necessary permissions. Contact your system administrator for this task.

   The **Delete Tags** dialog box appears to confirm that you want to delete the tag.

4. Click **Delete** on the confirmation dialog box.

   The tag is removed from the database and no longer appears on the Tags page.

CAUTION: If you have assigned a tag that you are deleting with any object, no warning message is displayed before the deletion of the tag. When you delete a tag, Junos Space Network Management Platform removes the object-tag association and the tag is no longer associated with any object. The deletion of a tag does not delete any tagged objects.

You can delete a tag not only from the Tags workspace but also from other workspaces such as the Device Management inventory landing page or the Job Management page.

To delete a tag from the Device Management inventory landing page:

1. On the Junos Space Network Management Platform user interface, select **Devices** > **Device Management**.

   The Device Management page appears.

2. If tags are not displayed, click the **Display Tag View** icon on the toolbar.

3. Select a tag and click **Delete Tag** from the shortcut menu.

   This option is disabled if you do not have sufficient permissions to delete the selected tags. This situation may arise when you are trying to delete a public tag for which you do not have the necessary permissions. Contact your system administrator for this task.

   A confirmation dialog box appears to confirm whether you want to delete the tag.

4. Click **Yes** on the confirmation dialog box.

   The tag is removed from the database and no longer appears on the Tags page.

CAUTION: If you have assigned the tag that you are deleting to any object, no warning message is displayed before the deletion of the tag. When you delete a tag, Junos Space Network Management Platform removes the object-tag association and the tag is no longer associated with any object. The deletion of the tag does not delete any tagged objects.

When you delete a tag, an audit log entry is automatically generated.

RELATED DOCUMENTATION

- Tags Overview | **1506**
- Managing Tags | **1512**
- Sharing a Tag | **1521**
- Renaming Tags | **1522**
- Creating a Tag | **1507**

Tagging an Object

You can create user-defined tags on an application workspace inventory page to easily categorize and organize managed objects. Subsequently, you can view and use these tags to easily search for multiple objects to view the status or perform a bulk action on them without having to select each object individually.

By default, the tags that you create from any workspace are private tags and these private tags are visible only to you. If you want any other user to use the tag that you created, then you have to create a pubic tag instead of a private tag or convert the private tag to a public tag.

To tag an object:

1. Navigate to an application workspace manage inventory page. For example, select **Devices** > **Device Management**.

2. Select the inventory objects that you want to tag.

3. Select **Tag It** from the Actions menu.

   The **Apply Tag** dialog box appears.

4. Select or type the tag name in the field.

   If you have existing tags, start to type a tag name in the name field. Existing tags appear in the selection box.

   You can also type a new tag name in the field. The new tag is automatically created and applied to the selected objects.

5. (Optional) Select the **Make Public** check box to mark the new tag created in the previous step as a public tag. If you do not select this check box, the new tag added is classified as a private tag.

   > **NOTE:** If you do not have permissions to create a public tag, then the **Make Public** check box is disabled.

6. (Optional) Add a comment in the **Add Description here** field.

7. Click **Apply Tag**. This action tags the object and stores the tag in the database.

RELATED DOCUMENTATION

Tags Overview | 1506
Managing Tags | 1512
Viewing Tags for a Managed Object | 1532
Untagging Objects | 1527
Filtering the Inventory by Using Tags | 1528
Creating a Tag | 1507

Untagging Objects

Starting with Junos Space Network Management Platform Release 15.2R1, you can untag or remove a tag from objects on an inventory page. You can select one or more objects at a time to untag.

To untag objects:

1. Navigate to the inventory page. For example, select **Devices** > **Device Management**.

2. Select the objects that you want to untag, then select **UnTag It** from the Actions menu. Alternatively, right-click the objects that you want to untag and select **UnTag It**.

   The **UnTag Objects** dialog box appears.

   > **NOTE:** All the tags that are associated with the selected objects are displayed. If there are no tags that are common to all the selected objects, a warning message indicating that no common tags are found is displayed above the list of tags.

3. Select the tags that you want to remove.

4. Click **Untag**.

   The Untag dialog box appears, displaying a message indicating that the selected tags have been successfully removed.

5. Click **OK**.

   You are returned to the inventory page. In this example, you are returned to the Device Management inventory page.

Release History Table

Release	Description
15.2R1	Starting with Junos Space Network Management Platform Release 15.2R1, you can untag or remove a tag from objects on an inventory page. You can select one or more objects at a time to untag.

RELATED DOCUMENTATION

- Tags Overview | **1506**
- Managing Tags | **1512**
- Tagging an Object | **1526**
- Viewing Tags for a Managed Object | **1532**
- Creating a Tag | **1507**

Filtering the Inventory by Using Tags

You can use tags to filter objects on a workspace inventory page. Filtering allows you to view only the objects that you want to categorize by tag name.

To filter the inventory by using a tag:

1. On the workspace inventory page, click the magnifying glass in the search field at the top-right of the page. You can also type the first letter of the tag name on the search field.

   A list appears with object names at the top and tag names at the bottom. (If you typed a letter in the search field, only the tag names starting with that letter appear.)

2. Click a tag name on the list.

   Only the inventory objects with that tag name appear. You see Filtered By the tag name at the top-left of the page.

3. Click the red **X** to remove the filtering from the inventory page.

In another aspect of filtering, on some pages, you can preview the tagged objects that you selected. For example, in the Configuration Files workspace, in **Configuration Files > Config Files Management > Backup Config Files**, you can select devices by tags. This form of filtering enables you to verify that you are performing the current operation on the correct objects.

RELATED DOCUMENTATION

Tags Overview | 1506
Managing Tags | 1512
Tagging an Object | 1526
Viewing Tags for a Managed Object | 1532
Untagging Objects | 1527
Creating a Tag | 1507

Viewing Tagged Objects

The **View Tagged Objects** page in the **Administration** workspace displays the list of objects that are associated with a tag.

NOTE:

- Users who are logged in to the Global domain can view public tags and private tags that they created, and tagged objects. However, only users with administration privileges can create or share public tags and view private tags of other users.
- Subdomains do not support tag administration tasks.

To view objects that are associated with a tag:

1. On the Junos Space Network Management Platform user interface, select **Administration** > **Tags**.

   The Tags page appears displaying the existing tags.

2. Select the tag for which you want to view the associated objects, and from the Actions menu, select **View Tagged Objects**. (Alternatively, right-click a tag and select **View Tagged Objects** or click the hyperlink corresponding to the **Tagged Object Count** column.)

   The View Tagged Objects page, which is divided into two panes, appears. The left pane displays the category (sorted alphabetically) and the right pane displays information, as shown in Table 191, about the tagged objects. By default, the first category is selected.

   Table 191: Tagged Objects

Field	Description	Supported Action
Name	Name of the tagged object	Sorting and filtering
Domain	Domain to which the tagged object belongs	Sorting and filtering

Table 191: Tagged Objects *(continued)*

Field	Description	Supported Action
Description	Description of the tagged object	Sorting

NOTE:

- Click the button next to a field to access the menu for sorting, displaying columns, and filtering.
- The total object count for the selected category is displayed at the top of the page. When the object count is high, use the GUI controls at the bottom of the page to manage the number of objects that are displayed or to navigate to a specific page.
- Only the list of objects supported for tagging, as shown in Table 192, are displayed on the right pane. When you click a category that has tagged unsupported objects, an error message is displayed.

3. (Optional) Select a category on the left pane of the View Tagged Objects page to view the objects that are associated with the selected category.

4. To return to the Tags page, click **Back** on the upper left of the View Tagged Objects page.

Table 192: List of Supported Objects

Category or Workspace	Object Type	Object Details
Device Management	**Devices**	• **Name**—Hostname of the device • **IP Address**—IP address of the device
Device Management	**Deployment instances**	• **Name**—Name of the deployment instance • **Description**—Description of the deployment instance
Device Templates	**Template definitions**	• **Name**—Name of the template definition • **Description**—Description of the template definition
Device Templates	**Templates**	• **Name**—Name of the template • **Description**—Description of the template
CLI Configlets	**Configlets**	• **Name**—Name of the configlet • **Description**—Description of the configlet
CLI Configlets	**Configuration View**	• **Name**—Name of the configuration view • **Description**—Description of the configuration view

Table 192: List of Supported Objects *(continued)*

Category or Workspace	Object Type	Object Details
CLI Configlets	**Configuration Filter**	• **Name**—Name of the configuration filter • **Description**—Device family with which the configuration filter is associated
CLI Configlets	**XPath and Regex**	• **Name**—Name of the XPath or regular expression • **Description**—Property type of the XPath or regular expression
Images and Scripts	**Scripts**	• **Name**—Name of the script • **Description**—Description of the script
Images and Scripts	**Images**	• **Name**—Name of the image • **Description**—Description of the image
Images and Scripts	**Operations**	• **Name**—Name of the operation • **Description**—Description of the operation
Images and Scripts	**Script Bundle**	• **Name**—Name of the script bundle • **Description**—Description of the script bundle
Report Management	**Report Definition**	• **Name**—Name of the report definition • **Description**—Description of the report definition
Report Management	**Generated Reports**	• **Name**—Name of the generated report • **Description**—Description of the generated report
Configuration Files	**Config Files Management**	• **Name**—Name of the configuration file • **Description**—Name of the device associated with the configuration file
Job Management	**Job Instance**	• **Jobs**—Name of the job • **Description**—Owner and state of the job
Role Based Access Control	**User Accounts**	• **Username**—Name of the user • **Description**—First name and last name of the user
Role Based Access Control	**Roles**	• **Name**—Name of the role • **Description**—Description of the role
Administration	**Fabric**	• **Name**—Name of the node • **Description**—IP address and status of the node
Administration	**Applications**	• **Name**—Name of the application • **Description**—Application version

Table 192: List of Supported Objects *(continued)*

Category or Workspace	Object Type	Object Details
Administration	**DMI Schemas**	• **Name**—Name of the device family • **Description**—Device series and OS version

RELATED DOCUMENTATION

Tagging an Object | **1526**

Tags Overview | **1506**

Managing Tags | **1512**

Viewing Tags for a Managed Object

The View Tags action from application workspace inventory pages allows you to see all tags that you have assigned to a managed object on your network. You must first tag a managed object to see its tags.

Use tags to label and categorize objects in your network, such as subnets, devices, services, users, customers, and so forth, so you can filter, monitor, or perform batch actions on them without having to select each object individually.

Tags created by you are private and visible only to you unless you have the Tag Administrator share them to the public domain, making them public. Tags created by other users are visible only to them unless the Tag Administrator shares them, then including you can view them.

To view tags on an inventory object:

1. Navigate to a workspace inventory page.

2. Select only one inventory object for which you want to view tags.

3. Select **View Tags** from the Actions menu. You can also right-click an object and select **View Tags**.

   The **View Tags** dialog box appears with a tag list displaying all tags applied to the selected object.

4. Click **OK**.

RELATED DOCUMENTATION

Managing Tags | 1512
Tagging an Object | 1526
Untagging Objects | 1527

Exporting Tags from Junos Space Network Management Platform

You export tags from the Junos Space Network Management Platform database to access the details of the tags. You can download the tags in CSV format to your local computer.

To export tags from Junos Space Platform:

1. On the Junos Space Network Management Platform user interface, select **Administration > Tags**.

   The Tags page that appears displays all tags that currently exist in the Junos Space Platform database.

2. Select the check boxes next to the tags that you want to export and click **Export Tags** on the toolbar.

   The Export Tags dialog box that appears displays the tags that you selected.

3. Click **Export** and save the CSV files to your local computer.

   The Export Tags Job Status dialog box displays the status of the export tags job.

   Close the dialog box to return to the Tags page.

RELATED DOCUMENTATION

Tags Overview | 1506
Managing Tags | 1512

CHAPTER 82

Managing DMI Schemas

IN THIS CHAPTER

- DMI Schema Management Overview | 1534
- Viewing and Managing DMI Schemas | 1536
- Viewing Missing DMI Schemas | 1538
- Setting a Default DMI Schema | 1540
- Configuring Access to Juniper Networks DMI Schema Repository by Using the Configure SVN Repository Action | 1541
- Adding Missing DMI Schemas or Updating Outdated DMI Schemas in Junos Space Network Management Platform | 1543
- Creating a Compressed TAR File for Updating DMI Schema | 1553
- Viewing and Deleting Unused DMI Schemas | 1557

DMI Schema Management Overview

Junos Space Network Management Platform interfaces with network devices using an open API called the Device Management Interface (DMI), which is a standard interface used by Juniper Networks devices. The DMI schema for a device describes the complete configuration and operational capabilities of the device OS version. DMI schemas are available at the Juniper Networks DMI schema repository, which you can access by going to https://xml.juniper.net/dmi/repository/trunk/ and logging in using your Juniper Networks support credentials.

You must manage the DMI schemas in Junos Space Platform if you want to use the full functionality of configuration management features available. You manage DMI schemas in Junos Space Platform by using the DMI Schemas page (**Administration** > **DMI Schemas**). Using the DMI Schemas page, you can view the existing DMI schemas installed, update DMI schemas, view missing schemas, set a schema as the default for a specific device family, and delete unused schemas.

NOTE: Because configuration management in Junos Space Platform is implemented using DMI schema, you can support most new device Junos OS versions by updating just the schema.

Each device type is described by a unique data model (DM) that contains all the configuration data for the device. The DMI schema lists all the possible fields and attributes for a type of device. The newer schemas describe the new features coming out with recent device releases. It is important that you load all your device schemas into Junos Space Platform; otherwise, only a default schema is applied when you try to edit a device configuration by using the device configuration edit action in the Devices workspace (see "Modifying the Configuration on the Device" on page 322). If Junos Space Platform has exactly the right DMI schema for each of your devices, you can access all configuration options specific to each device.

For every device family, one DMI schema is marked as the default schema. By default, the default schema is used when you create device templates. However, you can choose to use another schema when creating a template definition. In addition, when you modify a device configuration by using the Schema-based configuration editor, access to all configuration options for the device are available only if the DMI schema specific to the device is available in Junos Space Platform. If the schema version in use is close to the version of Junos OS running on the device, then most of the configurations options are still available.

NOTE:

- You can update schemas directly from the Juniper Networks DMI schema repository or upload a compressed TAR file containing the DMI schemas into Junos Space Platform.
- It is preferable that you install device schemas pertaining only to the devices that are currently managed from Junos Space Platform. When more devices are managed, you can install the device schemas that are relevant to the newly added devices.
- Starting from Release 17.1R1, Junos Space Platform provides options to automatically download missing schemas or update outdated schemas during device synchronization. For information about downloading device schema automatically from the DMI schema repository, see "Configuring Access to Juniper Networks DMI Schema Repository by Using the Configure SVN Repository Action" on page 1541 and "Adding Missing DMI Schemas or Updating Outdated DMI Schemas in Junos Space Network Management Platform" on page 1543 .

Release History Table

Release	Description
17.1R1	Starting from Release 17.1R1, Junos Space Platform provides options to automatically download missing schemas or update outdated schemas during device synchronization. For information about downloading device schema automatically from the DMI schema repository, see "Configuring Access to Juniper Networks DMI Schema Repository by Using the Configure SVN Repository Action" on page 1541 and "Adding Missing DMI Schemas or Updating Outdated DMI Schemas in Junos Space Network Management Platform" on page 1543

RELATED DOCUMENTATION

Setting a Default DMI Schema | 1540

Troubleshooting the Nondisplay of the DMI Schema Tree Issue | 1652

Device Discovery Profiles Overview | 220

Adding Missing DMI Schemas or Updating Outdated DMI Schemas in Junos Space Network Management Platform | 1543

Viewing and Managing DMI Schemas

You use the DMI Schemas page (in the Administration workspace) to view and manage multiple Device Management Interface (DMI) schemas for device families running Junos OS.

To view and manage DMI schemas:

1. On the Junos Space Network Management Platform user interface, select **Administration** > **DMI Schemas**.

   The DMISchemas page appears displaying the existing DMI schemas. For each schema, the device family, OS version, device series, state, and type are displayed, as shown in Table 193.

   You can sort the schemas based on the different fields (by clicking the corresponding column); in addition, you can choose which columns are displayed.

   Table 193: Information About DMI Schemas

Field	Description	Location
Device Family	Device family to which the schema belongs; for example, junos, junos-es, or junos-qfx	DMI Schemas page DMISchema Details dialog box Quick View
OS Version	Version of the device OS	DMI Schemas page DMI Schema Details dialog box Quick View
Device Series	Device series for which the schema is applicable	DMI Schemas page DMI Schema Details dialog box

Table 193: Information About DMI Schemas *(continued)*

Field	Description	Location
State	Indicates whether the DMI schema is a default for the respective device family	DMI Schemas page DMI Schema Details dialog box Quick View
Schema Installed **NOTE:** Starting from Junos Space Platform Release 17.1R1, the Type column is changed to Schema Installed on the DMI Schemas page.	Indicates whether the DMI schema for a Junos OS version on a device series is installed in Junos Space Platform Yes indicates that schema is installed in Junos Space Platform	DMI Schema Details page Quick View

2. (Optional) Double-click a row (or select a row and click the **View Schema Details** icon or right-click and select **View Schema Details**) to view additional information about the selected schema.

   The **DMI Schema Details** dialog box is displayed. For information about the fields displayed in this dialog box, see Table 193.

   Click **Close** to close the dialog box and return to the DMI Schemas page.

   NOTE: You can also select a row in the table and click the Quick View icon on the toolbar to toggle the quick view. For information about the fields displayed in the quick view, see Table 193.

3. (Optional) Select a schema and click **View Tags** from the Actions menu (or the shortcut menu) to view the tags associated with that schema.

   The **View Tags** dialog box displays the following information for each tag associated with the schema:

   - **Tag Name**—Name of the tag
   - **Access Type**—Indicates whether the tag is public or private

   Click **OK** to close the dialog box and return to the DMI Schemas page.

You can perform the following actions on the DMI Schemas page:

- Update (Add) a DMI schema—For more information, see ."Adding Missing DMI Schemas or Updating Outdated DMI Schemas by Using the Update Schema Menu" on page 1548
- View missing schemas—For more information, see "Viewing Missing DMI Schemas" on page 1538.
- Set a schema as a default—For more information, see "Setting a Default DMI Schema" on page 1540.
- Configure access to Juniper Networks DMI Schema repository—For more information, see "Configuring Access to Juniper Networks DMI Schema Repository by Using the Configure SVN Repository Action" on page 1541
- Download the latest schema from the Juniper Networks DMI Schema repository—For more information, see "Adding Missing DMI Schemas or Updating Outdated DMI Schemas in Junos Space Network Management Platform" on page 1543
- Add missing schemas—For more information, see "Adding Missing DMI Schemas or Updating Outdated DMI Schemas in Junos Space Network Management Platform" on page 1543
- View and delete unused schemas—For more information, see "Viewing and Deleting Unused DMI Schemas" on page 1557.
- Tag and untag schemas, and delete private tags—For more information, see "Tags Overview" on page 1506.

Release History Table

Release	Description
17.1R1	Starting from Junos Space Platform Release 17.1R1, the Type column is changed to Schema Installed on the DMI Schemas page.

RELATED DOCUMENTATION

Creating a Compressed TAR File for Updating DMI Schema | 1553

DMI Schema Management Overview | 1534

Viewing Missing DMI Schemas

In Junos Space Network Management Platform, you can view the list of Device Management Interface (DMI) schemas that are missing. Missing schema versions are the OS versions on devices that Junos Space Platform discovers in your network, but are not installed on Junos Space Platform. When schema versions are missing in Junos Space Platform, we recommend that you install the missing schema versions. However, installing a schema is not critical if the version of the schema already installed in Junos Space Platform is close to the versions of Junos OS running on the devices.

To view missing DMI schemas :

1. On the Junos Space Platform user interface, select **Administration** > **DMI Schemas**.

   The DMISchemas page appears.

2. From the Actions or the shortcut menu, select **View/Install Missing Schemas**.

   The **View/Install Missing Schemas** dialog box appears displaying a list of schemas that are not installed in Junos Space Platform. For each schema, the device family and OS version are displayed.

   If there are no missing schemas, then the list is empty.

   > **NOTE:** Starting from Junos Space Platform Release 17.1R1, the View Missing Schema action is changed to View/Install Missing Schema.

3. Click **Close** to close the dialog box.

   You are taken to the DMI Schemas page.

Release History Table

Release	Description
17.1R1	Starting from Junos Space Platform Release 17.1R1, the View Missing Schema action is changed to View/Install Missing Schema.

RELATED DOCUMENTATION

- Setting a Default DMI Schema | **1540**
- Adding Missing DMI Schemas or Updating Outdated DMI Schemas in Junos Space Network Management Platform | **1543**
- Configuring Access to Juniper Networks DMI Schema Repository by Using the Configure SVN Repository Action | **1541**

Setting a Default DMI Schema

In Junos Space Network Management Platform, a device family always has a default DMI schema associated with it. Typically, when you perform a clean installation of Junos Space Platform, a schema (usually the latest one) is automatically set as the default for each device family. When you perform an upgrade of Junos Space Platform, the default schemas stay the same as the ones before the upgrade.

NOTE:

- When you create a device template definition, Junos Space Platform uses a default DMI schema for the device family unless you select a schema.
- The schema that Junos Space Platform uses for a device family depends on the schema versions installed on Junos Space Platform and on the version of the device OS. The criteria that Junos Space Platform uses for picking a schema is as follows:
  - If an exact matching schema is available, then that schema is used irrespective of whether it is the default (for the device family) or not.

    An exact match refers to the case when the schema family and OS version are the same as the device family and the OS version running on the device.
  - If an exact matching schema is not available, the default schema for the device family is used.

    This ensures that even if an exact matching schema is not available, the default schema is used for managed devices belonging to a specific device family.

To set a default DMI schema :

1. On the Junos Space Platform user interface, select **Administration** > **DMI Schemas**.

   The **DMI Schemas** page appears displaying the available schemas.

2. Select the schema that you want to set as the default, then from the Actions or shortcut menu, select **Set Default Schema**.

   The **Set Default DMI Schema** dialog box appears, displaying the DMI schema name , device family, and OS version.

3. Click **Set Default**.

   The schema that you selected is set as the default and you are taken to the DMI Schemas page.

   The **State** field for the default schema displays **default**.

RELATED DOCUMENTATION

DMI Schema Management Overview | 1534

Adding Missing DMI Schemas or Updating Outdated DMI Schemas by Using the Update Schema Menu | 1548

Modifying the Configuration on the Device | 322

Troubleshooting the Nondisplay of the DMI Schema Tree Issue | 1652

Configuring Access to Juniper Networks DMI Schema Repository by Using the Configure SVN Repository Action

Starting from Junos Space Network Management Platform release 17.1R1, you can configure the Juniper Networks DMI schema repository (https://xml.juniper.net/dmi/repository/trunk/) by using the Configure SVN Repository action. The Auto Install Schema check box on the SVN Access Configuration dialog box, which when selected, allows Junos Space Platform to automatically download and install or update DMI schemas from the configured DMI Schema repository.

To configure access to the Juniper Networks DMI schema repository by using the Configure SVN Repository action:

1. On the Junos Space Platform user interface, select **Administration** > **DMI Schemas**.

   The DMI Schemas page appears.

2. From the Actions or the shortcut menu, select **Configure SVN Repository**.

   The SVN Access Configuration dialog box is displayed.

3. In the **SVN URL** field, enter the URL of the Juniper Networks DMI schema repository (https://xml.juniper.net/dmi/repository/trunk/).

4. In the **User Name** field, enter the user name to access the Juniper Networks DMI schema repository.

5. In the **Password** field, enter the password to access the Juniper Networks DMI schema repository.

6. In the **Confirm** field, reenter the password to access the Juniper Networks DMI schema repository.

7. (Optional) The **Proxy Server** field displays whether a proxy server is configured or not. If your organization requires that you use a proxy server to connect to the Internet, you must configure and enable the proxy server (under **Administration** > **Proxy Server**) before connecting to the Juniper

Networks DMI schema repository. For more information, see "Configuring Proxy Server Settings" on page 1502.

8. (Optional) Select the **Auto Install Schema** check box to automatically install any missing device schema or get the latest version of schema available in the Juniper Networks DMI schema repository during device synchronization.

   NOTE: When the Auto Install Schema text box is selected, Junos Space Platform identifies the DMI schemas that are missing or that need update during device synchronization. The missing schemas are installed and outdated schemas in Junos Space Platform are updated when the job, scheduled to run every one hour, fetches the schemas from the DMI repository.

   If a schema is missing and auto-installation of the schema fails, no attempt to install the schema is made when the job runs the next time.

9. (Optional) Click **Test Connection**.

   A message dialog box appears (after a few seconds or a few minutes depending on the connection) to indicate whether the connection is established successfully or not. Click **OK** to close the dialog box and return to the **SVN Access Configuration** dialog box.

10. Click **Save** to save the settings that you configured.

Release History Table

Release	Description
17.1R1	Starting from Junos Space Network Management Platform release 17.1R1, you can configure the Juniper Networks DMI schema repository (https://xml.juniper.net/dmi/repository/trunk/) by using the Configure SVN Repository action. The Auto Install Schema check box on the SVN Access Configuration dialog box, which when selected, allows Junos Space Platform to automatically download and install or update DMI schemas from the configured DMI Schema repository.

RELATED DOCUMENTATION

DMI Schema Management Overview | 1534

Adding Missing DMI Schemas or Updating Outdated DMI Schemas in Junos Space Network Management Platform | 1543

Adding Missing DMI Schemas or Updating Outdated DMI Schemas in Junos Space Network Management Platform

IN THIS SECTION

- Adding Missing DMI Schemas by Using the View/Install Missing Schema Action | **1543**
- Adding Missing DMI Schemas or Updating Outdated DMI Schemas by Using the Get Latest Action | **1544**
- Adding Missing DMI Schemas or Updating Outdated DMI Schemas by Using REST APIs | **1544**
- Adding Missing DMI Schemas or Updating Outdated DMI Schemas by Using the Update Schema Menu | **1548**

When a new device is added to your network, you need to add the DMI schema for that device to Junos Space Platform to configure and manage the device. You can view whether the schema for a device series is installed or not on Junos Space Platform from the DMI Schemas page. A value of No in the Schema Installed column indicates that the schema for a Junos OS version on a device series is not present in Junos Space Platform.

You can download DMI schema from the configured Juniper Networks DMI schema repository to Junos Space Platform in one of the following ways:

Adding Missing DMI Schemas by Using the View/Install Missing Schema Action

Junos Space Platform provides the View/install Missing Schema action to view and install DMI schemas that are missing from Junos Space Platform.

To add missing schemas by using the View/Install Missing schemas action:

1. On the Junos Space Platform interface, select **Administration > DMI Schemas**.

   The DMI Schemas page appears.

2. Select **Actions > View/Install Missing Schemas**.

   The View/Install Missing Schemas page lists the device family and the OS versions for which schemas are not present in Junos Space Platform.

3. Select the device family and OS versions for which you want to download schemas, and click **Install**.

   A job to download the selected schemas is initiated and the Job ID is displayed.

4. (Optional) Click the Job ID link to view the job details.

If the job is successful, the job details displays the number of schemas successfully installed and the number of schemas that could not be installed.

The job may fail if connection to the DMI schema repository is broken or if the required schema is not present in the repository.

Adding Missing DMI Schemas or Updating Outdated DMI Schemas by Using the Get Latest Action

The Get Latest action downloads missing schemas and updates outdated schemas in Junos Space Platform. The Get Latest action is enabled only after the DMI schema repository is configured.

To add or update schemas by using the Get Latest action:

1. On the Junos Space Platform interface, select **Administration > DMI Schemas**.

   The DMI Schemas page appears displaying the existing DMI schemas.

2. Select one or more DMI schemas

3. Select **Actions > Get Latest**.

   A job is created to download the schemas from the DMI schema repository and the job ID is displayed. If a DMI schema is already present in Junos Space Platform and outdated, the schema is overwritten by the latest schema downloaded from the DMI schema repository. If the DMI schema is not present in Junos Space Platform,, the schema is downloaded from the repository and installed in Junos Space Platform.

4. (Optional) Click the job ID to view the job details.

   The Job Details page displays if the Get Latest action was successful or not.

Adding Missing DMI Schemas or Updating Outdated DMI Schemas by Using REST APIs

Junos Space Platform provides an option to download missing schemas or update outdated schemas by using REST APIs for situations where the Junos Space Platform is not connected to the Web.

To generate the APIs, Junos Space Platform has the **schemaInstall.py** script stored in the **/var/log/space-debug/debug-utilities/schemaManagement** location. When Junos Space Platform is not connected to the Web, download the script to a local system from which you can connect to the Web. The information for using the **schemaInstall.py** script to manage DMI schemas is documented in this section and is also present in the **ReadMe.txt** file located at **/var/log/space-debug/debug-utilities/schemaManagement**.

To run the **schemaInstall.py** script on a local system, the local system should meet the following requirements:

- Python 3.6 (https://www.python.org/ftp/python/3.6.1/python-3.6.1.exe)
- SVN client such as Tortoise SVN (https://tortoisesvn.net/downloads.html)
- Python Installation Package (PIP) Version 3.6 installed on the local system

> **NOTE:** You can obtain help for the **schemaInstall.py** script by using the **python schemaInstall.py --help** command.

You can run the **schemaInstall.py** script as follows to add missing schemas or update outdated schemas in Junos Space Platform depending on connectivity of the local system to Junos Space Platform and the DMI schema repository:

> **NOTE:** Before you run the script, copy the script to a local system that is connected to the Web.

The following variables are used by the **schemaInstall.py** script:

- *svnurl* is the link to DMI Schema repository (https://xml.juniper.net/dmi/repository/trunk/).
- *spaceuser* is the username for logging in to Junos Space Platform.
- *svnuser* is the username for logging in to the DMI Schema repository.
- *spaceurl* is the link to Junos Space Platform.
- **Situation 1:** When your local system is connected to both Junos Space Platform and the DMI schema repository, you can execute the script to perform the following tasks:
  - Add missing DMI schemas in Junos Space Platform by executing the following command on the local system:

    ```
    python schemaInstall.py -o install-missing-schemas --svnurl="<svnurl>"
    --spaceuser="<spaceuser>" --svnuser="<svnuser>" --spaceurl="<spaceurl>"
    ```

  - Add specific schemas on Junos Space platform by executing the following command on the local system:

    ```
    python schemaInstall.py -o install-schemas --svnurl="<svnurl>"
    --spaceuser="<spaceuser>" --svnuser="<svnuser>" --spaceurl="<spaceurl>"
    --file="schema.xml"
    ```

    Where, ***schema.xml*** is the file containing specific schemas that you want to install.

```
~~ Structure of sample schema.xml file ~~

<dmi-schema-infos
uri="/api/space/schema-service/dmi-schemas-with-missing-schemas">
     <dmi-schema-info>
         <os-version>3.0R1</os-version>
         <dev-family>ive-ic</dev-family>
     </dmi-schema-info>
     <dmi-schema-info>
         <os-version>11.3X30.10</os-version>
         <dev-family>junos-qf</dev-family>
     </dmi-schema-info>
</dmi-schema-infos>
```

You can obtain the **schema.xml** file by one of the following means:

- Create the schema file manually.
- Obtain the list of all schemas present in Junos Space Platform by executing the following command:

```
 python schemaInstall.py -o get-schemas --spaceurl="<spaceurl>"
--spaceuser="<spaceuser>" --file="schema.xml"
```

- Obtain the list of schemas missing in Junos Space Platform by executing the following commands:

```
python schemaInstall.py -o checkout-missing-schemas --svnurl="<svnurl>"
--spaceuser="<spaceuser>" --svnuser="<svnuser>" --spaceurl="<spaceurl>"
```

The **schema.xml** file obtained by using the **get-schemas** and the **checkout-missing-schemas** methods can be used for installing schemas on Junos Space Platform and checking out schemas on the DMI Schema repository.

- Find the schemas missing in Junos Space Platform and obtain those schemas from the DMI schema repository in a ***.tgz** file by executing the following command:

```
python schemaInstall.py -o checkout-missing-schemas --svnurl="<svnurl>"
--spaceuser="<spaceuser>" --svnuser="<svnuser>" --spaceurl="<spaceurl>"
```

This command outputs the **upload-tgz-schema-file.tgz** archive file. You can upload the archive file later by using the Update Schema menu; see "Adding Missing DMI Schemas or Updating Outdated DMI Schemas by Using the Update Schema Menu" on page 1548 for details.

- **Situation 2:** When the local system has connectivity to the DMI schema repository but not to the Junos Space platform, you can execute the script to download specific schemas in archived format (***.tgz**) from the repository. You can later add the schemas to Junos Space Platform by using the Update Schema

menu; see “Adding Missing DMI Schemas or Updating Outdated DMI Schemas by Using the Update Schema Menu” on page 1548 for details.

```
python schemaInstall.py -o checkout-schemas --svnurl="<svnurl>"
--svnuser="<svnuser>" --file="schema.xml"
```

- **Situation 3:** When the local system is connected to Junos Space Platform, but not to the DMI Schema repository, you can do the following:
  - Upload archived schema to Junos Space Platform by executing the following command:

    ```
    script python schemaInstall.py -o install-schemas --spaceuser="<spaceuser>"
    --spaceurl="<spaceurl>" --archivefile="upload-tgz-schema-file.tgz"
    ```

    where, ***upload-tgz-schema-file.tgz*** is the name of the archived schema file uploaded to Junos Space Platform.

    > **NOTE:** You can obtain the **upload-tgz-schema-file.tgz** file by downloading it from the DMI repository and copying it to the local system.

Adding Missing DMI Schemas or Updating Outdated DMI Schemas by Using the Update Schema Menu

You can add (update) a Device Management Interface (DMI) schema in the following ways by using the Update Schema menu:

- By uploading an existing compressed TAR file (extension **.tgz** or **.tar.gz**) containing the DMI schema into Junos Space Network Management Platform

  > **NOTE:** You can create your own compressed TAR file (see "Creating a Compressed TAR File for Updating DMI Schema" on page 1553) or obtain the file by contacting the Juniper Networks Technical Assistance Center (.

- By downloading the DMI schema from the Juniper Networks DMI schema repository containing DMI schemas

  > **NOTE:** The Juniper Networks DMI schema repository (https://xml.juniper.net/dmi/repository/trunk) does not currently support IPv6. If you are running Junos Space on an IPv6 network, you can do one of the following:
  >
  > - Configure Junos Space to use both IPv4 and IPv6 addresses and download the DMI schema by using the Junos Space Network Management Platform Web GUI.
  > - Download the DMI schema by using an IPv4 client and create the compressed TAR file and update or install the DMI schema by using the Junos Space Web GUI.

To update a DMI schema on Junos Space Network Management Platform:

1. On the Junos Space Network Management Platform user interface, select **Administration** > **DMI Schemas**

   The DMI Schemas page appears.

2. Click the **Update Schema** icon on the toolbar.

   The **Update Schema** page appears.

   > **NOTE:** On the Update Schema page, Junos Space Platform displays the schemas that you already have installed and, based on the discovered devices, suggests new schemas. However, you can pick other available schemas and download them.

3. Perform one of the following actions:

- To update the DMI schema from an existing compressed TAR file:

  a. Select the **Local (tgz)** option button.

  b. Click **Browse**.

     The **File Upload** dialog box appears.

  c. Select the compressed TAR file and click **Open**.

     The Update Schema page reappears, displaying the compressed TAR file in the **Local Schemas File** field.

  d. Click **Upload**.

     > **NOTE:** Do not navigate away from the Update Schema page while the compressed TAR file is being uploaded to Junos Space Platform. The time taken for the upload process depends on the number of schemas in the file. A progress bar indicates the percentage of the upload that has completed.

- To update the DMI schema directly from the Juniper Networks DMI schema repository:

  a. Select the **Juniper Repository** option button.

     If the access to the Juniper Networks DMI schema repository is already configured, the URL of the repository is displayed in the **URL** field. If the access is not configured, a note indicating that the access must be configured is displayed.

     To configure access to the Juniper Networks DMI schema repository:

     i. Click **Configure**.

        The **Juniper Access Configuration** dialog box appears.

     ii. In the **Juniper URL** field, (https://xml.juniper.net/dmi/repository/trunk/) appears by default.

     iii. In the **User Name** field, enter the user name to access the Juniper Networks DMI schema repository.

     iv. In the **Password** field, enter the password to access the Juniper Networks DMI schema repository.

v. In the **Confirm** field, reenter the password to access the Juniper Networks DMI schema repository.

vi. (Optional) The **Proxy Server** field displays whether a proxy server is configured or not. If your organization requires that you use a proxy server to connect to the Internet, you must configure and enable the proxy server (under **Administration** > **Proxy Server**) before connecting to the Juniper Networks DMI schema repository. For more information, see "Configuring Proxy Server Settings" on page 1502.

vii. (Optional) Select the **Auto Install Schema** check box to automatically download any missing device schema or the latest version of any outdated schema from the DMI schema repository during device synchronization.

> **NOTE:** When the Auto Install Schema text box is selected, Junos Space Platform identifies the DMI schemas that are missing or that need update during device synchronization. The missing schemas are installed and outdated schemas in Junos Space Platform are updated when the job, scheduled to run every one hour, fetches the schemas from the DMI repository.
>
> If a schema is missing and auto-installation of the schema fails, no attempt to install the schema is made when the job runs the next time.

viii. (Optional) Click **Test Connection**.

A message dialog box appears (after a few seconds or a few minutes depending on the connection) to indicate whether the connection is established successfully or not. Click **OK** to close the dialog box and return to the **Juniper Access Configuration** dialog box.

ix. Click **Save** to save the settings that you configured.

You are taken to the Update Schema page and the URL that you configured is displayed in the **URL** field.

b. (Optional) From the **Device Family** drop-down list, select the device families that you want to download from the repository.

> **NOTE:** If you do not specify a device family, then available schemas from all families are listed.

c. Click **Connect**.

Junos Space Platform displays a message asking you to wait while the list of schemas is retrieved. (This process might take anywhere from a few seconds to a few minutes depending on the connection.)

The available DMI schemas are displayed in a table under the **Schema Availability** label, as shown in Table 194.

You can sort the schemas based on a specific column, choose which fields are displayed, or filter the list of schemas displayed.

Table 194: Information Displayed About Available Schemas

Column	Description
Device Family	Name of the device family to which the DMI schema belongs; for example, junos-ex
Release	Junos OS release version to which the DMI schema corresponds
Date	Date on which the DMI schema was published If you uploaded a compressed TAR file, this field displays **Unknown**.
Available	Indicates whether the schema is available (in the compressed TAR file or the Juniper Networks DMI schema repository) or not
Installed	Indicates whether the schema is already installed on Junos Space or not
Missing	Indicates whether the schema is a missing schema or not Missing schema versions are the OS versions on devices that Junos Space Platform discovers in your network, but have not been installed on Junos Space Platform.

4. (Optional) To overwrite a previously existing schema, select the **Enable Schema Overwrite** check box.

   By default, the DMI schemas that are previously installed are listed and are disabled. However, when you select this check box, you can select these schemas to be overwritten by the schemas from the repository or from your local system.

5. (Optional) To display only recommended schemas, select the **Show recommended schemas only** check box.

6. (Optional) To schedule a time for installing the DMI schema, select the **Schedule at a later time** check box and specify the date and time in the **Date and time** field.

7. Select the schemas from the list of schemas displayed in the table by clicking the check box corresponding to a schema.

   NOTE: If you have chosen to update only schemas for specific device families, then only those schemas belonging to the specific device families are listed.

8. Click **Install**.

   The Install DMI Schema Information dialog box appears displaying the job ID.

   NOTE: You can verify the status of the job by clicking the hyperlinked job ID in the Install DMI Schema Information dialog box. You are taken to the Job Management page.

9. Click **OK**.

   You are taken to the DMI Schemas page. After the DMI schema is installed, this page displays the newly installed schemas.

NOTE:

- Updating a schema automatically generates an audit log entry.
- You must set at least one schema as the default schema for each device family in your network. This is done automatically by Junos Space Platform as long as there is at least one schema for the device family. For more information, see "Setting a Default DMI Schema" on page 1540.

RELATED DOCUMENTATION

DMI Schema Management Overview | **1534**

Troubleshooting the Nondisplay of the DMI Schema Tree Issue | **1652**

Viewing Missing DMI Schemas | **1538**

Creating a Compressed TAR File for Updating DMI Schema

IN THIS SECTION

- Creating a Compressed Tar File on Linux | 1553
- Creating a Compressed Tar File on Microsoft Windows | 1554
- Schemas Available in Junos Space Platform | 1556

This topic contains instructions for creating a compressed tar file (extension **.tgz** or **.tar.gz**) on Linux or Microsoft Windows. You use the compressed tar file to update a DMI schema on Junos Space Network Management Platform (see "Adding Missing DMI Schemas or Updating Outdated DMI Schemas by Using the Update Schema Menu" on page 1548).

Before you create a compressed tar file, ensure the following:

- The internal directory structure of the compressed tar file complies with the following format; that is, when you extract the compressed tar file, all files must be extracted to a folder structured as follows: **dmi/*deviceFamily*/releases/*osVersion*/....**
- The compressed tar file has the **.tgz** or **.tar.gz** extension.
- You have the username and password for xml.juniper.net, which are your Juniper Networks support credentials.

> **NOTE:** In this topic, we provide examples that contain only HTTPS URLs. However, both HTTP and HTTPS URLs are supported. If the repository (whose URL is being entered) supports both HTTP and HTTPS access, we recommend that you use an HTTPS URL.

This topic contains the following sections:

Creating a Compressed Tar File on Linux

To create a compressed tar file (for updating DMI schema) on Linux:

1. Install the Subversion (SVN) client on Linux. To install Subversion client on Linux, refer to Installing Subversion or other relevant documentation.

2. Create a temporary directory.

3. Navigate to the temporary directory created in the preceding step.

4. Check out the files from Subversion by executing the following command:

   svn --username=*userName* --password=*userPwd* co *dmiRepositoryURL*

   where *userName* and *userPwd* are the username and password required to access xml.juniper.net , and ***dmiRepositoryURL*** is the URL of the repository folder that you want to checkout.

   Examples of the DMI respository URLs are shown in Table 195.

   Table 195: Sample URLs for the Repository

Type	Example URL
For the whole Junos OS family	https://xml.juniper.net/dmi/repository/trunk/junos
For a device family	https://xml.juniper.net/dmi/repository/trunk/junos-es/
For a selected OS version	https://xml.juniper.net/dmi/repository/trunk/junos-ex/releases/11.2R2.4/

5. Tar the **dmi** directory by executing the following command from within the directory containing the **dmi** directory:

   tar czvf *filename* dmi

   where *filename* is the same of the compressed tar file. You can use any filename as long as the extension of the file is **.tgz** or **.tar.gz**

The compressed tar file is now ready for uploading into Junos Space Platform.

Creating a Compressed Tar File on Microsoft Windows

To create a compressed tar file (for updating DMI schema) on Microsoft Windows:

1. Install the Subversion (SVN) client on Microsoft Windows from the following location: https://tortoisesvn.net/ .

   NOTE: To install the Subversion client, you can also use any software or tool that is equivalent to TortoiseSVN.

2. Install 7-Zip to generate a compressed tar file on Microsoft Windows by using the following link: http://www.7-zip.org/ .

   NOTE: To generate the compressed tar file, you can also use any software or tool that is equivalent to 7-Zip.

3. Create a temporary folder.

   NOTE: You can use any name for the temporary folder.

4. Create a folder called **dmi** within the previously created temporary folder.

5. Right-click the **dmi** folder and select **SVN Checkout**:

   A dialog box is displayed.

6. In the **URL of repository** field, enter the full URL of the repository. Refer to Table 195 for examples of URLs that you can enter.

7. In the **Checkout directory** field, enter the full path of the checkout directory; for example, **C:\test\dmi\junos-es**.

   NOTE: The portion of the path to the right of the **dmi** folder must be equivalent to the corresponding portion after **trunk** in the URL of the repository. For example, if the repository URL is https://xml.juniper.net/dmi/repository/trunk/junos-es/ the checkout directory path is **C:\test\dmi\junos-es**, and if the repository URL is https://xml.juniper.net/dmi/repository/trunk/junos-es/releases/10.1R3/, the checkout directory path is **C:\test\dmi\junos-es\releases\10.1R3**.

8. In the **Checkout depth** field, enter **Fully recursive**.

9. Ensure that the **Omit externals** check box is cleared.

10. Select **HEAD revision**.

11. Click **OK**, and if you are prompted to, provide credentials.

    The files are checked out from the Subversion repository into the specified folder.

12. Create the tar file from the **dmi** folder using 7-Zip:

    a. Right-click the **dmi** folder and select **7-Zip**.

    b. Click **Add to Archive**.

    c. In the **Archive Format** field, select **tar**.

    d. Click **OK**

13. Compress the tar file file using 7-Zip:

    a. Right-click the **dmi.tar** file and select **7-Zip**.

    b. Click **Add to Archive**.

    c. In the **Archive Format** field, select **gzip**.

    d. Click **OK**

14. (Optional) Rename the ***.tar.gz** file to ***.tgz**

The compressed tar file is now ready for uploading into Junos Space Platform.

Schemas Available in Junos Space Platform

Table 196 displays information about the schemas available for use in Junos Space Network Management Platform.

Table 196: Schema Name Mapping Information

Schema Family	Device Family Series
junos	ACX Series/J Series/M Series/MX Series/T Series/TX Series/PTX Series/EX92xx Series
junos-es	J Series/SRX Series/LN Series

Table 196: Schema Name Mapping Information *(continued)*

Schema Family	Device Family Series
junos-ex	EX Series
media-flow	Junos Content Encore
junos-qfx	QFX Series
junos-qf	QF
bxos	BXOS
tcaos	TCA Series

RELATED DOCUMENTATION

- DMI Schema Management Overview | 1534
- Adding Missing DMI Schemas or Updating Outdated DMI Schemas by Using the Update Schema Menu | 1548
- Setting a Default DMI Schema | 1540
- Viewing and Deleting Unused DMI Schemas | 1557

Viewing and Deleting Unused DMI Schemas

From the Administration workspace, you can delete any unused Device Management Interface (DMI) schemas that no longer need to be managed by Junos Space Network Management Platform. A schema is considered unused if it meets both of the following conditions:

- The schema is not associated with a device, a template, or a template definition.
- The schema is not set as the default schema for any device family.

NOTE:

- You can delete any unused schema from Junos Space Platform if you are a user who is assigned the privileges of a Super Administrator or System Administrator.
- When you delete a schema, Junos Space Platform automatically generates an audit log entry.

To view and delete unused schemas:

1. On the Junos Space Platform user interface, select **Administration** > **DMI Schemas**.

   The DMI Schemas page appears.

2. From the Actions menu, select **View/Delete Unused Schemas**.

   The **View/Delete Unused Schemas** dialog box appears displaying a list of unused schemas in a table. For each schema, the device family and OS version are displayed.

   If there are no unused schemas, then Junos Space Platform displays the message **Unused schemas do not exist in Space** in a dialog box. Click **OK** to close the dialog box.

3. Select the schemas that you want to delete.

4. Click **Delete** to delete the selected schemas.

   The **Delete Unused Schemas** dialog box appears and a message that a job to delete the schemas is triggered is displayed along with the hyperlinked job ID.

   The selected schemas are deleted from the Junos Space Platform database; in addition, the relevant files on the nodes in the fabric are deleted.

   > **NOTE:** You can click the hyperlinked job ID to view the status of the job on the Job Management page. On the Job Management page, the Summary column for the job displays the number of schemas that were successfully deleted and the number of schemas that were not deleted from the list of selected schemas.
   >
   > If the schemas were not deleted, you can double-click the job to view the reasons for failure.

5. Click **OK**.

   You are taken to the DMI Schemas page. After the schema deletion job is successfully completed, the deleted schemas are no longer visible on this page.

RELATED DOCUMENTATION

Viewing and Managing DMI Schemas | **1536**

Setting a Default DMI Schema | **1540**

CHAPTER 83

Managing Hardware Catalog

IN THIS CHAPTER

- Hardware Catalog Overview | 1559
- Viewing Information About Hardware Catalog | 1561
- Configuring Access to Juniper Networks Subversion Repository for Downloading Hardware Catalog | 1561
- Uploading Hardware Catalog to Junos Space Network Management Platform | 1563

Hardware Catalog Overview

Starting from Release 17.1R1, Junos Space Network Management Platform provides Hardware Catalog that enable you to manage hardware components of Juniper Networks devices. Hardware catalog saves you from updating Junos Space Platform software every time a new hardware component, for example, a line card, an FPC, or a power supply module, is added to a Juniper Networks device that Junos Space Platform manages. When new components are added, Juniper Networks provides a new hardware catalog that you can import to the Junos Space platform.

You can extend Junos Space Platform support to new hardware components on managed devices by uploading the latest hardware catalog distributed in the ***.tgz** archived format by Juniper Networks or downloaded from the Juniper Networks subversion (SVN) repository to Junos Space Platform. .

> **NOTE:** Hardware catalog does not enable fault and performance monitoring of newly added hardware components on managed devices.

The content of the hardware catalog is derived from the latest DMI schema and always includes the latest hardware components present in the devices running Junos OS. The hardware catalog archive also contains a **readme.txt** file that includes the revision number and the date and time of publishing the catalog. The following is a sample of the **readme.txt** file:

```
Revision:02
Published:Wed Mar 09 1:30:00 IST 2017
Last Updated:Fri Mar 10 2:12:00 IST 2017
```

You can view and manage hardware catalogs from the Hardware Catalog page of the Junos Space Platform user interface. From the Hardware Catalog page, you can also configure the settings for downloading hardware catalogs from Juniper Networks SVN repository.

The Hardware Catalog page displays the following information:

- revision number of the hardware catalog installed in Junos Space Platform
- the date and time the hardware catalog was initially published by Juniper Networks
- the date and time the hardware catalog in Junos Space Platform was last updated
- the revision number and the date and time since the latest hardware catalog is available in the SVN repository

You can perform the following tasks on the Hardware Catalog page:

- View details of the hardware catalog ; see "Viewing Information About Hardware Catalog" on page 1561 for details.
- Upload a hardware catalog to the Junos Space Platform; see "Uploading Hardware Catalog to Junos Space Network Management Platform" on page 1563 for deails.
- Configure the SVN repository settings for downloading hardware catalogs; see "Configuring Access to Juniper Networks Subversion Repository for Downloading Hardware Catalog" on page 1561 for details.

Release History Table

Release	Description
17.1R1	Starting from Release 17.1R1, Junos Space Network Management Platform provides Hardware Catalog that enable you to manage hardware components of Juniper Networks devices. Hardware catalog saves you from updating Junos Space Platform software every time a new hardware component, for example, a line card, an FPC, or a power supply module, is added to a Juniper Networks device that Junos Space Platform manages. When new components are added, Juniper Networks provides a new hardware catalog that you can import to the Junos Space platform.

RELATED DOCUMENTATION

Device Inventory Overview | 299

Device Management Overview | 189

Viewing Information About Hardware Catalog

You can view the revision numbers of hardware catalog present in the Juniper Networks Subversion (SVN) repository and Junos Space Platform and on the Hardware Catalog page.

To view information about the hardware catalog present in the SVN repository and Junos Space Platform, on the Junos Space Platform user interface, select **Administration > Hardware Catalog**. The Hardware Catalog page appears.

The Hardware Catalog page displays the following information about the hardware catalog currently present in Junos Space Platform under the Current Hardware Catalog section:

- Revision—The revision number of the hardware catalog.
- Published—The date and time the hardware catalog was initially published.
- Last Updated—The date and time the hardware catalog in Junos Space Platform was last updated.

Click the **Refresh SVN Info** button under the Hardware Catalog in SVN section to fetch the revision number of the current hardware catalog in the SVN repository.

The Hardware Catalog page displays the following information about the hardware catalog present in the SVN repository under the Hardware Catalog in SVN section:

- SVN Revision—The revision number of the hardware catalog about the hardware catalog in the SVN repository.
- Published—The date and time the current revision of the hardware catalog was published

RELATED DOCUMENTATION

Hardware Catalog Overview | **1559**

Uploading Hardware Catalog to Junos Space Network Management Platform | **1563**

Configuring Access to Juniper Networks Subversion Repository for Downloading Hardware Catalog | **1561**

Configuring Access to Juniper Networks Subversion Repository for Downloading Hardware Catalog

If you want to download the latest hardware catalog from the Juniper Networks SVN repository, configure the SVN Repository settings from the Hardware Catalog page.

To configure the repository to download hardware catalog:

1. On the Junos Space Network Management Platform user interface, select **Administration > Hardware Catalog.**

   The Hardware Catalog page appears.

2. Click **Configure** under the Hardware Catalog in SVN section.

   The Configure SVN Access dialog box appears.

3. Enter the following details in the Configure SVN Access dialog box:
   - SVN Url—URL of the SVN server (https://xml.juniper.net/space/repository/trunk/hardware-catalog/)
   - User Name—Username of a customer's Juniper Networks account
   - Password—Password of a customer's Juniper Networks account
   - Confirm—Retype the password
4. (Optional) The Proxy Server field displays whether a proxy server is configured or not. If your organization requires that you use a proxy server to connect to the Internet, you must configure and enable the proxy server (under Administration > Proxy Server) before connecting to the Juniper Networks SVN repository. For more information, see Configuring Proxy Server Settings.

5. (Optional) Click **Test Connection** to check whether you are able to connect to the SVN server.

   If the connection is successful, the **Connection established** message is displayed. If the connection fails, the **Cannot establish connection. Please check the proxy setting or your network connection** message is displayed.

   The Refresh SVN Info and the Get Latest buttons are enabled after you are connected to the SVN server.

6. Click **Save** to save or **Cancel** to cancel the SVN repository configuration.

RELATED DOCUMENTATION

Hardware Catalog Overview | **1559**

Viewing Information About Hardware Catalog | **1561**

Uploading Hardware Catalog to Junos Space Network Management Platform | **1563**

Uploading Hardware Catalog to Junos Space Network Management Platform

IN THIS SECTION

- Updating Hardware Catalog in Junos Space Platform by Using the Get Latest Action | **1563**
- Uploading Hardware Catalog to Junos Space Platform by Using the Import Option | **1564**

When a new hardware catalog is available, you can obtain the catalog from Juniper Networks subversion (SVN) repository after configuring the SVN repository. Alternatively, you can also upload the hardware catalog manually to Junos Space Platform..

Updating Hardware Catalog in Junos Space Platform by Using the Get Latest Action

Juniper Networks updates the hardware catalog in the Juniper Networks subversion (SVN) repository so that you can configure the SVN repository on Junos Space Platform and download the latest version of the hardware catalog. For information about configuring SVN repository to download hardware catalog, see"Configuring Access to Juniper Networks Subversion Repository for Downloading Hardware Catalog" on page 1561.

Ensure that the SVN repository is configured on Junos Space Platform before you perform the Get Latest action. For information about configuring the SVN repository.

To update hardware catalog in Junos Space Platform:

1. On the Junos Space Network Management Platform user interface, select **Administration > Hardware Catalog**.

   The Hardware Catalog page appears.

2. Click **Get Latest** under the Hardware Catalog in SVN section.

   The Get Latest Hardware Catalog from SVN dialog box appears.

   A job is initiated to download the latest hardware catalog present in the SVN server and the ID of the job is displayed.

3. (Optional) Click the Job ID to view the job details.

   The Job Details page displays whether the hardware catalog was uploaded successfully or not.

Uploading Hardware Catalog to Junos Space Platform by Using the Import Option

Junos Space Network Management Platform provides an option to manually upload the hardware catalog when Junos Space is not connected to the Juniper Networks SVN repository . Juniper Networks shares the hardware catalog with customers in the ***.tgz** format.

The hardware catalog files are available in .xml format. Click here to download the required XML files, create a file in ***.tgz**, and upload it using the Import option. The ***.tgz** file must have the following structure to upload the hardware catalog successfully.

Sample *.tgz File Format

```
[user@nm-apps-ip27 junos-ex]$ tar -tvf hwctlg.tgz
drwxrwxr-x user/user   0 2017-06-21 19:10 hardware-catalog/
-rw-rw-r-- user/user 1637 2017-06-21 19:10 hardware-catalog/EX2200-48P-4G.xml
-rw-rw-r-- user/user 1637 2017-06-21 19:10 hardware-catalog/EX2200-24T-4G.xml
-rw-rw-r-- user/user 1109 2017-06-21 19:10 hardware-catalog/EX2200-12P-2G.xml
-rw-rw-r-- user/user 1637 2017-06-21 19:10 hardware-catalog/EX2200-24P-4G.xml
-rw-rw-r-- user/user 1109 2017-06-21 19:10 hardware-catalog/EX2200-12T-2G.xml
```

Before you begin upload of hardware catalog by using the Import option, save the hardware catalog in the ***.tgz** format on your local system or on a network drive.

You can either download the hardware catalog from the Juniper Networks SVN repository or contact Juniper Networks support to obtain it.

To upload hardware catalog to Junos Space Platform by using the Import option:

1. On the Junos Space Platform user interface, select **Administration > Hardware Catalog**.

   The Hardware Catalog page appears.

2. Click **Browse** to locate the hardware catalog file on your local system.

   NOTE: The file to be uploaded should in be in the ***.tgz** format.

3. Click **Import** to import the hardware catalog file to Junos Space Platform.

A job is initiated to import the hardware catalog and the ID of the job is displayed. The hardware catalog file is imported to **/var/jboss/jmp-tmp/net/juniper/jmp/var/hw-catalog** location on the Junos Space server.

4. (Optional) Click the Job ID to view the job details.

   The Job Details page displays whether the hardware catalog was imported successfully or not.

RELATED DOCUMENTATION

- Hardware Catalog Overview | **1559**
- Configuring Access to Juniper Networks Subversion Repository for Downloading Hardware Catalog | **1561**
- Viewing Information About Hardware Catalog | **1561**

CHAPTER 84

Managing the Purging Policy

IN THIS CHAPTER

- Junos Space Purging Policy and Purging Categories Overview | 1566
- Viewing the Junos Space Purging Policy and Purging Criteria | 1567
- Modifying the Purging Policy and Purging Criteria and Setting the Policy Status | 1569

Junos Space Purging Policy and Purging Categories Overview

Junos Space Network Management Platform provides a built-in purging policy that enables you to purge backup files, logs, and other resources on the Junos Space server, and free system resources. The purging policy provided by Junos Space Platform is also a framework for purging that Junos Space applications can use to specify files and logs to be purged in application-specific locations.

The following categories can be purged:

- Configuration files—Backup device configuration files in the **/var** directory
- Reports—Generated reports in the **/var** directory
- Database backup files—Database backup files in the **/var** directory
- Troubleshooting log files—Troubleshooting log files in the **/var/cache/jboss/space-logs** directory
- Other log files—Log files mainly in the **/var/log/** directory with the filenames ***.log.***, **messages.***, or **SystemStatusLog.***

A user with System Administrator or Super Administrator privileges (or a custom user with the Purging Policy task assigned) can view and modify purging criteria and trigger conditions for Junos Space Platform and, if configured, for installed applications. In addition, the user can enable or disable purging categories and view detailed information about the purging job on the Job Management page.

> **NOTE:** The **Purging Policy** task (in the Role Based Access Control workspace) comprises the subtasks **Modify Purging Policy**, **Edit Purging Category**, and **Set Policy Status**.

Purging is triggered when one of the following conditions is met in the following order of priority:

1. When the specified percentage threshold of disk usage is exceeded—Junos Space monitors the **/var** and **/var/log** partitions every five minutes by using a **cron** job and triggers a purging job if the threshold is crossed for *any* of the purging categories.

   NOTE:
   - When the **/var** partition exceeds the specified disk threshold percentage, files are purged in the following decreasing order of priority: Database backup files > Reports and Troubleshooting log files > Configuration files.
   - In all partitions, the files are purged only until the disk threshold percentage is exceeded; when the disk threshold percentage for a particular partition falls below the specified value, the purging is stopped.
   - For a purging policy triggered by a **cron** job:
     - If the Junos Space fabric is configured with MySQL on one or two dedicated database nodes, the database backup files and log files (mainly in the **/var/log/** directory with the filenames ***.log.***, **messages.***, or **SystemStatusLog.***) are not purged from the dedicated database nodes.
     - If the Junos Space fabric is configured with one or two FMPM nodes,the log files (mainly in the **/var/log/** directory with the filenames ***.log.***, **messages.***, or **SystemStatusLog.***) are not purged from the FMPM nodes.

2. When the scheduled (recurring or nonrecurring) purging job is due.

   NOTE: The purging job is applicable only to the purging categories on which the purging policy is enabled.

RELATED DOCUMENTATION

Viewing the Junos Space Purging Policy and Purging Criteria | **1567**

Modifying the Purging Policy and Purging Criteria and Setting the Policy Status | **1569**

Viewing the Junos Space Purging Policy and Purging Criteria

On the Purging Policy page, users with the role Super Administrator or System Administrator (or a custom user with the Purging Policy task assigned) can view the built-in purging policy and view and modify purging

criteria and trigger conditions for Junos Space Network Management Platform and, if configured, for installed applications. In addition, users can enable or disable purging categories and view detailed information about the purging job on the Job Management page.

To view the purging policy, purging criteria, and trigger conditions:

1. On the Junos Space Platform UI, select **Administration** > **Purging Policy**.

   The Purging Policy page is displayed.

   This page displays the following trigger conditions for purging on the top part of the page (under **Trigger conditions for purging**):

   - **Disk usage threshold (%)**—Percentage of the disk space after which the files are purged
   - **Schedule at a later time**—Date and time at which the purging is scheduled
   - **Recurrence**—Interval at which the purging recurs

   The purging categories and criteria, as shown in Table 197, are displayed in a table on the bottom part of the page. You can sort the table by purging category, policy status, or priority.

Table 197: Purging Categories and Criteria

Field	Description
App Name	Junos Space application to which the purging category belongs; for Junos Space Platform, **Network Management Platform** is displayed.
Purging Category	Name of the purging category. The following purging categories are supported: • **Config File**—Backup device configuration files • **Reports**—Generated reports • **DB Backup**—Database backup files • **Space Logs**—Junos Space log files • **Troubleshooting Log**—Troubleshooting log files
Retention Criteria	Retention criteria for the purging category The period for which the records or files to be retained and the number of records or files to be retained are displayed.
Last Job ID	ID of the last job for the corresponding purging category Click the *job ID* link to view the details of the job on the Job Management page.

Table 197: Purging Categories and Criteria *(continued)*

Field	Description
Policy Status	Status of the purging policy for the corresponding purging category: • **Enabled**—Indicates that the purging policy is enabled for the category • **Disabled**—Indicates that the purging policy is disabled for the category When a purging category is disabled, Junos Space does not purge the files or records for that category.
Partition	Disk partition for the purging category from which the files or records are purged
Priority	Priority for the purging category A purging category with priority **High** has precedence over a purging category with priority **Medium**, which in turn has precedence over a category with priority **Low**.
Description	Description of the purging category

You can modify some of the fields on the Purging Policy page. For more information, refer to "Modifying the Purging Policy and Purging Criteria and Setting the Policy Status" on page 1569.

RELATED DOCUMENTATION

Junos Space Purging Policy and Purging Categories Overview | 1566

Modifying the Purging Policy and Purging Criteria and Setting the Policy Status

IN THIS SECTION

- Modifying the Purging Trigger Conditions | 1570
- Modifying the Purging Criteria and Enabling or Disabling a Policy | 1572

On the Purging Policy page, users with the role Super Administrator or System Administrator (or a custom user with the Purging Policy task assigned) can modify purging criteria and trigger conditions and enable

or disable purging categories for Junos Space Network Management Platform and, if configured, for installed applications.

To modify the purging policy and criteria, and set the policy status:

1. On the Junos Space Platform UI, select **Administration** > **Purging Policy**.

   The Purging Policy page appears displaying the trigger conditions for purging on the top part of the page (under **Trigger conditions for purging**) and the purging categories and criteria on the bottom part of the page.

   You can modify the purging trigger conditions and some fields related to the purging criteria and policy status.

This topic has the following sections:

Modifying the Purging Trigger Conditions

On the Purging Policy page, you can modify the trigger conditions for purging.

To modify the purging trigger conditions:

1. (Optional) In the **Disk usage threshold (%)** field, enter the percentage of the disk space that can be used beyond which the files are purged.

   When the percentage of the disk space used in the **/var** or **/var/log** partition exceeds the configured value, Junos Space triggers an intermediate purging job for the purging categories that are enabled and for which the disk usage threshold exceeds the configured limit. The purging job is executed based on the priority; the highest priority sub-job is executed first and after its completion, Junos Space Platform checks the disk threshold again. If the disk usage threshold is higher than the configured limit, then the purging job is continued in decreasing order of priority. If the disk threshold is lower than the configured limit, the job is stopped.

   The minimum value is 1 and the maximum is 100; the default is 85 percent.

2. (Optional) To modify the purging schedule:

   a. Select the **Schedule at a later time** check box.

      NOTE: To trigger a purging job that will run immediately, clear the **Schedule at a later time** check box.

b. In the **Start** field, specify the date and time on which you want the purging to start.

3. (Optional) To specify the recurrence interval:

   a. Select the **Recurrence** check box.

   > **NOTE:** To remove the recurrence, clear the **Recurrence** check box.

   b. In the **Interval** field, specify the recurrence interval (in minutes, hours, days, weeks, months, or years) and the frequency of recurrence.

      The default interval is **Monthly**.

      If you specify an interval in weeks, months, or years, you can specify on which days the purging should recur. Additionally, if the interval is in weeks, the day on which you are specifying the recurrence is selected and disabled by default; you can specify additional days on which the purging should recur.

   c. In the **Ends on** field, specify a date and time after which the recurrence ends. Alternatively, if you want the purging to recur indefinitely, select **Never**.

      By default, the purging recurs indefinitely.

   > **NOTE:** Junos Space triggers a purging policy job based on the following:
   >
   > - If both the **Schedule at a later time** and **Recurrence** fields are not specified, Junos Space triggers a job that will run immediately.
   > - If the **Schedule at a later time** field is specified but the **Recurrence** field is *not* specified, Junos Space triggers a job that will run later at the specified schedule.
   > - If the **Recurrence** field is specified but the **Schedule at a later time** field is *not* specified, Junos Space triggers a job that will run immediately with the specified recurrence.
   > - If both the **Schedule at a later time** and **Recurrence** fields are specified, Junos Space triggers a job that will run later at the specified schedule and the specified recurrence.

4. After modifying the trigger conditions, you can perform one of the following actions:

   - Click **Save** to save the modifications that you made.
     - If you modified the trigger conditions and a purging policy job does not exist, a dialog box is displayed warning you that the trigger conditions will be updated and that a purging job will be created.

Click **Schedule** to save the changes and schedule the purging policy job.

- If you modified the trigger conditions and a purging policy job already exists, a dialog box is displayed warning you that the trigger conditions will be updated and that a purging job already exists.

  Click **Reschedule** to reschedule the existing purging job.

  The job is rescheduled and the purging policy page is reloaded.

- Click **Discard** to discard the modifications that you made.

  The modifications are discarded and the settings are returned to the previous saved state. The Purging Policy page is reloaded.

Modifying the Purging Criteria and Enabling or Disabling a Policy

On the Purging Policy page, you can modify the purging criteria and enable or disable a purging policy.

To modify the purging criteria and enable or disable a purging policy:

1. Select the purging policy by clicking inside the row corresponding to a category.

   The selected purging policy is highlighted.

2. (Optional) To enable or disable the purging policy:

   a. Click the Set Policy Status button (check mark).

      A confirmation dialog box appears prompting you to confirm that you want to change the policy status.

   b. Click **Yes** to change the policy status.

      The policy status is changed and the Purging Policy page is reloaded; the **Policy Status** field displays the new status.

3. (Optional) To modify the purging criteria:

   NOTE: You cannot modify the name of a criterion but only its value.

   a. Click the Edit Purging Criteria (pencil icon) button.

      The Edit Purging Criteria page pops up. The name of the criterion and the corresponding value is displayed.

   b. Click the pencil icon next to the criterion or double-click the row that you want to modify.

The selected row expands and displays the **Criteria Name** field (disabled) and the **Value** field.

c. Enter the value for the criterion in the **Value** field.

d. Perform one of the following actions:

- Click **Save** to save the modification.

  The modification is saved, the expanded row is closed, and the modified value is displayed.

- Click **Cancel** to discard the modification.

  The modification is discarded, the expanded row is closed, and the previously saved value is displayed.

4. (Optional) To modify additional purging criteria, follow the procedure outlined in step 3.

5. Click **OK** to close the page.

   You are taken to the Purging Policy page.

RELATED DOCUMENTATION

Junos Space Purging Policy and Purging Categories Overview | **1566**

Monitoring and Troubleshooting Guide

PART 13

Overview

Overview | 1576

CHAPTER 85

Overview

IN THIS CHAPTER

- Monitoring Network Devices and Troubleshooting Software Issues with Junos Space Network Management Platform | **1576**
- Overall System Condition and Fabric Load History Overview | **1580**
- Junos Space Network Management Platform Widgets | **1583**

Monitoring Network Devices and Troubleshooting Software Issues with Junos Space Network Management Platform

IN THIS SECTION

- Systems of Record | **1577**
- System Snapshot | **1577**
- Backup and Restore | **1578**
- Maintenance Mode | **1578**
- Audit Logs | **1578**
- Jobs | **1579**
- Secure Console | **1579**
- Looking Glass | **1579**
- Reports | **1579**
- Junos Space Debug Utilities | **1580**

Use the following features of Junos Space Network Management Platform to monitor devices and troubleshoot software issues:

Systems of Record

A network managed by Junos Space Platform contains two repositories of information about the devices in the network: the devices themselves (each device defines and reports its official state) and the database (which contains information that is reported by the device during device discovery). This is known as systems of record.

The systems of record operate in the following two modes depending on where the repository of information is stored:

- Network as a system of record (NSOR)—By default, the network is the system of record (NSOR). In this mode, when a user commits a change in the configuration of a network device, the commit operation automatically triggers a report through the system log to Junos Space Platform.
- Junos Space as a system of record (SSOR)—In this mode, when you perform any out-of-band commit operation, Junos Space Platform receives a system log message from the device, but the values in the Junos Space Platform database are not automatically changed or synchronized with the values on the device. Instead, you can choose whether or not to overwrite the device's local changes by pushing the accepted configuration to the device from the Junos Space Platform database. For more information about systems of record in Junos Space Platform, see "Systems of Record in Junos Space Overview" on page 214.

System Snapshot

You can use the System Snapshot feature to create a snapshot of the current state of the Junos Space system. The snapshot includes all persistent data on the hard disk including data in the database, system and application configuration files, and application and Linux executables. You can roll back the Junos Space system to a predefined state or an older release if the system reaches an unrecoverable error state caused by undesirable behavior due to corruption of system files, interruption of critical processes, and so on. The System Snapshot is a fabric-wide operation that maintains consistency of data across all nodes in the fabric.

You can create a snapshot before a significant action is performed—for example, adding or deleting a Junos Space node, installing a Junos Space application, and so on—because the action can precipitate the system into an undesirable state. You can delete the snapshot after you have ascertained that the action was performed successfully. For more information about system snapshots, see "Creating a System Snapshot" on page 1279.

Backup and Restore

You use the Backup and Restore feature to back up (or schedule the backup of) and restore the data in the Junos Space database. You can set up an hourly, daily, or weekly schedule. The database backup can be stored on the local Junos Space system or transferred to a remote system automatically using the Secure Copy mechanism.

You can restore the backup in any of the following circumstances:

- Junos Space data is corrupted and you need to replace the corrupted data with uncorrupted data.
- Junos Space software is corrupted and unstable after a reinstallation or an upgrade and you need to populate the Junos Space database with uncorrupted data.

For more information about backup and restore operations, see "Backing Up and Restoring the Database Overview" on page 1305.

Maintenance Mode

Maintenance mode is a mode in which you can perform database restore and debugging tasks while all nodes in the fabric are shut down and the Junos Space Network Management Platform Web proxy is running. You need to be an authorized Junos Space administrator to put the system into maintenance mode. You can put the system into maintenance mode only after you initiate a restore task by using the Backup and Restore feature.

The Junos Space system goes into maintenance mode in the following situations:

- Junos Space Network Management Platform software goes down.
- You initiate a restore operation by using the Backup and Restore feature.
- You upgrade the Junos Space Network Management Platform software.

For more information about maintenance mode, see "Maintenance Mode Overview" on page 1153.

Audit Logs

The Audit Logs workspace of Junos Space Platform displays the login history and tasks initiated by a local or remote user. Through this workspace, you can track login history, view the list of device management tasks, view the list of services that were provisioned on the device, and so on. However, tasks that are not initiated by users, such as device-driven activities (for example, resynchronization of network elements), and changes made from the Junos Space CLI are not recorded in audit logs. Audit logs can be used by administrators to review events—for example, to identify which user accounts are associated with an event, to determine the chronological sequence of events (that is, what happened before and during an event), and so on. For more information about audit logs, see "Junos Space Audit Logs Overview" on page 1115.

Jobs

You use the Jobs workspace of Junos Space Platform to monitor the status of jobs that are run in Junos Space Platform and all Junos Space applications installed on Junos Space Platform. You can view the status of the jobs on the Job Management page. A job is a user-initiated action that is performed on any object that is managed by Junos Space Platform, such as a device, service, or customer. Typical jobs in Junos Space Network Management Platform include discovering devices, deploying services, prestaging devices, and performing functional and configuration audits.

You can trigger jobs immediately or schedule jobs for a later date and time. Junos Space Platform maintains a history of job statuses for all scheduled jobs. When a job is scheduled from a workspace, Junos Space Platform assigns a job ID that serves to identify the job on the Job Management page. For more information about jobs, see “Jobs Overview” on page 965.

Secure Console

The Secure Console feature on the Devices workspace provides a secure remote access connection to managed and unmanaged devices. Secure Console initiates an SSH session from the Junos Space user interface by using the SSH protocol. Secure Console is a terminal window embedded in Junos Space Platform that eliminates the need for a third-party SSH client to connect to devices. Secure Console provides additional security while connecting to your devices by initiating an SSH session from the Junos Space server rather than from your Web browser. You can access the Secure Console feature either from the Device Management page or the Secure Console page. For more information about Secure Console, see “Secure Console Overview” on page 396.

Looking Glass

You use the Looking Glass feature from the Devices workspace to view device configurations by executing basic CLI commands from the Junos Space user interface. You can execute these commands on multiple devices and compare the configurations and runtime information of these devices. You can execute the following types of commands by using Looking Glass: **show**, **ping**, **test**, and **traceroute**. The commands that are supported and stored in the Junos Space Platform database are displayed on the Looking Glass page. When you type the first few letters of the command, the suggestion list displays the commands that are supported, are stored, and begin with the letters that you typed. For more information about Looking Glass, see “Looking Glass Overview” on page 392.

Reports

With the Reports workspace of Junos Space Platform, you can generate customized reports for managing the resources in your network. You can use these reports to gather device inventory details, job execution details, user accounts, and audit trails. You first create a report definition to specify what information to retrieve from the Junos Space Platform inventory database. You then use this report definition to generate, export, and print the reports. Junos Space Platform provides some predefined categories to create report

definitions. You can combine multiple categories to create a report definition. By default, a predefined set of attributes is included in a report definition. You can choose to add or remove the attributes according to what information you want from the final generated report. You can group, sort, or filter data based on specific attributes available with the report definition. For more information about reports, see "Reports Overview" on page 768.

Junos Space Debug Utilities

Junos Space debug utilities are a collection of scripts and Java applications to fetch details that cannot be viewed on the JBoss CLI or from the Junos Space user interface. These scripts and Java applications are stored at **/var/log/space-debug/debug-utilities** and categorized under deviceConnection, jobManagement, deviceImport, and HornetQ directories. When you execute these scripts or Java applications, you can view details such as device-connection or node-connection issues, device XMLs fetched from the Junos Space Platform database, and jobs triggered and nodes that execute these jobs. For more information about Junos Space debug utilities, see "Junos Space Debug Utilities Overview" on page 1607.

RELATED DOCUMENTATION

Overall System Condition and Fabric Load History Overview | 1159

Junos Space Network Management Platform Widgets | 1583

Overall System Condition and Fabric Load History Overview

You can view the overall Junos Space system condition and fabric load from the Junos Space Network Management Platform Dashboard or the Administration statistics page.

Overall System Condition

To calculate the overall Junos Space system condition, Junos Space Platform uses a formula based on cluster health and node-function health:

- Cluster health indicates the percentage of nodes in the fabric that are currently running.

  For example, if only three nodes are reachable in a four-node fabric, cluster health is 75%.

- Load-balancer health indicates the percentage of nodes (enabled for load balancing) that are running the load-balancing process.

  For example, if two nodes are enabled for load balancing and the load-balancing process is running on only one node, the load-balancing health is 50%.

- Database health indicates the percentage of nodes (enabled for database requests) that are running the database process.

  For example, if two nodes are enabled as the database server and the database process is running on only one node, then database health is 50%.

- Application-logic health indicates the percentage of nodes (enabled for application logic (DML and business logic) that are running the application-logic process.

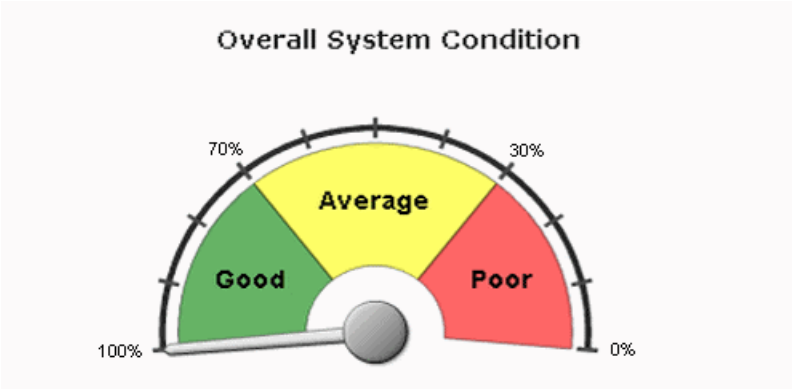
  For example, if three nodes are enabled for application logic and the application-logic process is running on only two nodes, then application-logic health is 67%.

Junos Space Platform retrieves data on the nodes and the node functions that are running, and then applies the following formula to determine the overall Junos Space system condition: Overall System Condition = [(Number of Nodes Running) / (Number of Nodes in Fabric)] * [(Number of Nodes Running Load_Balancing Process) / (Number of Nodes enabled for Load Balancing)] * [(Number of Nodes Running Database-Server Process) / (Number of Nodes Enabled As Database Server)] * [(Number of Nodes Running Application-Logic Process) / (Number of Nodes Enabled for Application Logic)]

The overall Junos Space system condition is expressed as a percentage. If we use the values in the preceding examples in this formula, then the overall system condition would be calculated as: Overall System Condition = 75% * 50%* 50% * 67% = 12.5%.

A value between 0 and 30% indicates that the system health is Poor, a value between 30% and 70% indicates that the system health is average, and a value between 70% and 100% indicates that the system health is good. The **Overall System Condition** chart displays the system health as shown in Figure 50

Figure 142: Overall System Condition Gauge



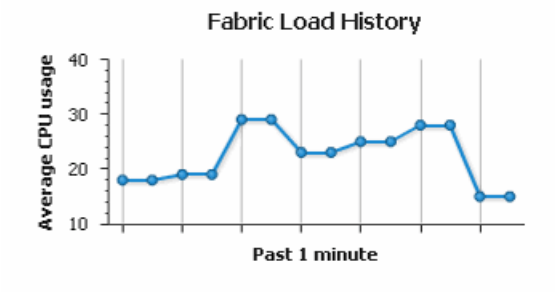
The overall system health indicates 0% (Poor) when any one of the following conditions is detected:

- No nodes in the fabric are running.
- No nodes enabled for load balancing are running the load-balancing process.
- No nodes enabled for database requests are running the database process.
- No nodes enabled for application logic are running the application-logic process.

Fabric Load History

The Fabric Load History chart, as shown in Figure 51, displays the average CPU usage across all nodes that are running in the fabric.

Figure 143: Fabric Load History Chart



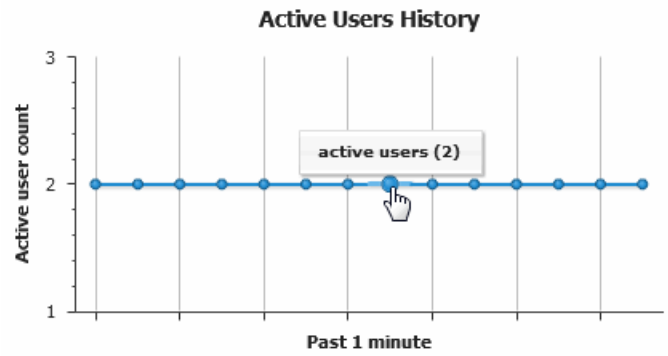
Junos Space Platform uses the following formula to determine the fabric load: Fabric Load = (Total CPU Usage for All Nodes Running) / (Number of Nodes Running)

For example, for a fabric with three nodes running and CPU usage of 80%, 30%, and 10%, respectively, the fabric load is 40%.

Active Users History

The Active Users History chart, as shown in Figure 52, displays the number of active users in the past one minute.

Figure 144: Active Users History Chart



RELATED DOCUMENTATION

Viewing the Junos Space Platform Dashboard | 126
Viewing the Administration Statistics | 1138

Junos Space Network Management Platform Widgets

IN THIS SECTION

- Devices | 1583
- Device Templates | 1584
- CLI Configlets | 1584
- Images and Scripts | 1584
- Reports | 1584
- Network Monitoring | 1585
- Configuration Files | 1585
- Jobs | 1585
- Role Based Access Control | 1586
- Audit Logs | 1586
- Administration | 1586

This topic presents a list of workspaces in Junos Space Network Management Platform and the widgets that they display:

Devices

The Devices workspace displays the following widgets:

- Device Count by Platform—Number of Juniper Networks devices added per device platform
- Device Status—Percentage of devices with the UP, Down, or NA connection status
- Device Count by OS—Number of devices running a particular Junos OS version
- Device Count by Synchronization State—Device discovery targets that were discovered, failed, are managed

For more information about these widgets, refer to the "Viewing Device Statistics" on page 446 topic in the *Junos Space Network Management Platform Workspaces Feature Guide*.

Device Templates

The Device Templates workspace displays the following widgets:

- Template Status—Percentage of device templates with the Enabled and Need Review statuses
- Template Definition Status—Percentage of device templates that are Published and Unpublished statuses
- Template Count by Device Family—Number of device templates created per device family

For more information about these widgets, refer to the "Viewing Device Template Statistics" on page 525 and "Viewing Template Definition Statistics" on page 524 topics in the *Junos Space Network Management Platform Workspaces Feature Guide*.

CLI Configlets

The CLI Configlets workspace displays the following widgets:

- CLI Configlet Count by Device Family—Number of CLI configlets created per device family
- Configuration Viewer Count by Device Family—Number of configuration views per device family

For more information about these widgets, refer to the "Viewing CLI Configlet Statistics" on page 552 and "Viewing Configuration Views Statistics" on page 595 topics in the *Junos Space Network Management Platform Workspaces Feature Guide*.

Images and Scripts

The Images and Scripts workspace displays the following widgets:

- Device Image Count by Platform Group—Number of device images per platform group
- Device Images Count by Version—Number of device images created per Junos OS version
- Number of Scripts by Type—Number of scripts created per script type. The script types are : Commit, Op, and Event
- Number of Jobs per Script Action—Number of jobs triggered by different script-related actions

For more information about these widgets, refer to the "Viewing Statistics for Device Images and Scripts" on page 610 topic in the *Junos Space Network Management Platform Workspaces Feature Guide*.

Reports

The Reports workspace displays the following widgets:

- Report Definition Count by User—Number of report definitions created per user
- Report Count by User—Number of reports created per user

For more information about these widgets, refer to the "Viewing Report Statistics" on page 795 and "Viewing Report Definition Statistics" on page 787 topics in the *Junos Space Network Management Platform Workspaces Feature Guide*.

Network Monitoring

The Network Monitoring workspace displays the following widgets:

- Nodes with Pending Problems—Nodes with outstanding alarms
- Nodes with Outages—Nodes that reported outages
- Availability Over the Past 24 hours—Number and percentage availability of the network interfaces of the devices that reported outages
- Notification—Check for notifications sent to you, all Junos Space Platform users, and the on-call schedule to fix outages.
- Resource Graphs—Search for resource graphs. Resource graphs display data collected from managed nodes throughout your network such as critical SNMP performance, response time, and so forth.
- KSC Reports—Search for key SNMP customized (KSC) reports. KSC reports enable you to create and view SNMP performance data using prefabricated graph types.
- Quick Search—Search for nodes by node ID, node label, IP address, or the type of service whether ICMP or SNMP.

For more information about these widgets, refer to the "Network Monitoring Reports Overview" on page 873 topic in the *Junos Space Network Management Platform Workspaces Feature Guide*.

Configuration Files

The Configuration Files workspace displays the following widgets:

- Configuration File Count by Device Family—Number of configuration files per device family
- Devices with most Frequently Revised Configuration Files—Devices whose configuration files have been revised most number of times

For more information about these widgets, refer to the "Viewing Configuration File Statistics" on page 940 topic in the *Junos Space Network Management Platform Workspaces Feature Guide*.

Jobs

The Jobs workspace displays the following widgets:

- Job Types—Percentage of all jobs of a particular type that are run
- State of Jobs Run—Percentages of jobs that succeeded, are canceled, are in progress, or failed

- Average Execution Time per Completed Job— Each bar in the Average Execution Time per Completed Job bar chart represents a job type and the average execution time in seconds.

For more information about these widgets, refer to the "Viewing Statistics for Jobs" on page 968 topic in the *Junos Space Network Management Platform Workspaces Feature Guide*.

Role Based Access Control

The Role Based Access Control workspace displays the following widget:

- Number of Users Assigned by Role—Percentage and the number of users that are assigned to a role

For more information about these widgets, refer to "Viewing User Statistics" on page 1068.

Audit Logs

The Audit Logs workspace displays the following widgets:

- Audit Log Statistical Graph—Tasks that are performed and logged in all Junos Space applications over a specific period of time
- Top 10 Active Users in 24 hours—Top ten users who performed the most number of tasks over 24 hours

For more information about these widgets, refer to the "Viewing Audit Log Statistics" on page 1121 topic in the *Junos Space Network Management Platform Workspaces Feature Guide*.

Administration

The Administration workspace displays the following widgets:

- System Health—Junos Space system condition, load on the fabric, and active users.
- System Alert Messages in the last 30 days—SMTP server alert messages categorized by application, and when the error last occurred.
- System Health Report—Health and performance of the Junos Space nodes in your Junos Space setup and the processes on these nodes. Staring in Release 15.2R1, the Administration workspace displays the System Health Report widget.

For more information about these widgets, refer to the "Viewing the Administration Statistics" on page 1138 topic in the *Junos Space Network Management Platform Workspaces Feature Guide*.

Release History Table

Release	Description
15.1R2	Staring in Release 15.2R1, the Administration workspace displays the System Health Report widget.

RELATED DOCUMENTATION

Overall System Condition and Fabric Load History Overview | 1159

Junos Space Debug Utilities Overview | 1607

PART 14

Log Files and Debug Utilities

Troubleshooting Junos Space Network Management Platform Issues by Using Log Files | **1589**

Troubleshooting Network Devices by Using Junos Space Debug Utilties | **1607**

CHAPTER 86

Troubleshooting Junos Space Network Management Platform Issues by Using Log Files

IN THIS CHAPTER

- System Status Log File Overview | **1589**
- Junos Space Network Management Platform Log Files Overview | **1591**
- Troubleshooting Log File Overview | **1595**
- Downloading the Troubleshooting Log File in Server Mode | **1596**
- Downloading the Troubleshooting Log File in Maintenance Mode | **1599**
- Downloading Troubleshooting System Log Files Through the Junos Space CLI | **1600**
- Customizing Node System Status Log Checking | **1605**
- Customizing Node Log Files to Download | **1606**

System Status Log File Overview

The system writes a system log file for each fabric node to provide troubleshooting and monitoring information. See "System Status Log File" on page 1408.

The System Administrator can customize the information that is collected in the system log file. See "Customizing Node System Status Log Checking" on page 1410.

The System Administrator can download the latest log files for each fabric node when logged in to a Junos Space Appliance. See "Downloading System Log Files for a Junos Space Appliance" on page 1409.

In each operating mode, the System Administrator can customize the default log files that are downloaded from a Junos Space Appliance. See "Customizing Node Log Files to Download" on page 1412.

System Status Log File

Approximately once a minute, the system checks and writes a status log file **SystemStatusLog** for each fabric node by default. Each log file consists of system status, such as the disk, CPU, and memory usage information, as shown. Junos Space Network Management Platform writes each system status log file to **/var/log/SystemStatusLog**

```
2009-08-10 11:51:48,673 DEBUG [net.juniper.jmp.cmp.nma.NMAResponse] (Thread-110:)
Node IP: 192.0.2.0Filesystem           1K-blocks      Used Available Use% Mounted
on
/dev/mapper/VolGroup00-LogVol00
                      79162184  15234764  59841252  21% /
Cpu(s):  8.7%us,  1.1%sy,  0.0%ni, 90.0%id,  0.1%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   3866536k total,  2624680k used,  1241856k free,    35368k buffers
Swap:  2031608k total,   941312k used,  1090296k free,   439704k cached
```

Customizing Status Log File Content

The System Administrator can customize the information that is written in a fabric node system status log file. For more information, see "Customizing Node System Status Log Checking" on page 1410.

Downloading System Log Files for a Junos Space Appliance

The System Administrator can download the latest log files for each fabric node when logged in to a Junos Space Appliance. The system status log file and all other third-party log files are collected and compressed in a troubleshooting file.

Table 181 lists the files included in the **troubleshoot** file.

Table 198: Log Files included in the troubleshoot File

Description	Location
System status log files	**/var/log/SystemStatusLog**
JBoss log files	**/var/log/jboss/***
Service-provisioning data files	**/var/tmp/jboss/debug/***
MySQL error log files	**/var/log/mysqld.log**
Log files for Apache, Node Management Agent (NMA), and Webproxy	**/var/log/httpd/***
Watchdog log files	**/var/log/watchdog/***
System messages	**/var/log/messages/***

The System Administrator can download log files in each operation mode as follows:

- Server mode (See "Downloading the Troubleshooting Log File in Server Mode" on page 1417.)
- Maintenance mode (See "Downloading the Troubleshooting Log File in Maintenance Mode" on page 1420.)

- CLI mode (See "Downloading Troubleshooting System Log Files Through the Junos Space CLI" on page 1421.)

Customizing Log Files to Download

The System Administrator can also customize the log files to be downloaded for specific fabric nodes. For more information about customizing node log files to download, see "Customizing Node Log Files to Download" on page 1412.

RELATED DOCUMENTATION

Customizing Node System Status Log Checking | **1410**

Customizing Node Log Files to Download | **1412**

Downloading the Troubleshooting Log File in Server Mode | **1417**

Downloading the Troubleshooting Log File in Maintenance Mode | **1420**

Downloading Troubleshooting System Log Files Through the Junos Space CLI | **1421**

Junos Space Network Management Platform Log Files Overview

IN THIS SECTION

- Apache Web Server Log Files | **1592**
- JBoss Application Server Log Files | **1592**
- MySQL Database Log Files | **1594**
- Node Management Agent Log Files | **1594**

Junos Space Network Management Platform log files contain useful information that help you to identify, analyze, and troubleshoot issues related to Junos Space Network Management Platform. The software components of Junos Space Network Management Platform—JBoss, Apache Web server, MySQL, and CentOS—generate these log files.

Table 199 lists log files related to the software components of Junos Space Network Management Platform.

Table 199: Junos Space Network Management Platform Log Files

Software Component	Description of the Log Files
Apache Web server	Log files from the Apache Web server, NMA, and Web proxy
JBoss	Log files from JBoss, Junos Space core, and hosted Junos Space applications
MySQL	Log files from MySQL servers
CentOS	Linux-based system log messages
Node Management Agent	Log files for system statuses and Junos Space and watchdog processes

In addition to the log files related to software components, you can also refer to the **/var/log/install.log** log file for information about Junos Space Platform upgrades and Junos Space application installations.

Apache Web Server Log Files

You can view the Apache Web server log files to view information related to HTTPS requests, Apache modules, and CGI programs.

Table 200 lists the Apache Web server log files.

Table 200: Apache Web Server Log Files

Log File	Description
/var/log/httpd/access_log	Logs related to incoming HTTPS requests
/var/log/httpd/error_log	Error logs for both Apache Web server modules and CGI programs
/var/log/httpd/ssl_error_log	Error logs related to SSL certificates

JBoss Application Server Log Files

JBoss is used as an application server in Junos Space Network Management Platform. It provides a runtime environment for plug-and-play Junos Space applications and supports standard packaging of pluggable applications based on the **.ear** file format. It also supports hot plug-and-play deployment of Junos Space applications when the system is fully operational.

JBoss provides three configuration options: minimal, default, and all. Junos Space Network Management Platform specifies **all** as the default JBoss configuration option.

Table 201 lists the JBoss directories.

Table 201: JBoss Directories

Type of JBoss Directory	JBoss Directory
Home directory	**/usr/local/jboss**
Log directory	**/var/log/jboss**
Data directory	**/var/spool/jboss**
tmp directory	**/var/tmp/jboss**

Table 202 lists the JBoss log files available in the **/var/log/jboss/servers/server1/** directory. You can also refer to the console file available in the **/var/log/jboss/** directory for console messages from JBoss.

Table 202: Joss Log Files

Log File Name	Description
boot.log	JBoss boot log file
console.log	Console log file
process-controller.log	Log file that contains records about starting and stopping services in domain mode
host-controller.log	Log file that contains information about the host controller that starts and stops the application server
provisioning.log	Service Provisioning application log file
server.log	JBoss Application server log file
long-jpa-txn.log	EJB transactions log file
Provisioning.log	Network Activate log file
Qos.log	QoS Design log file
SD.log	Security Director log file

The Junos Space Service Provisioning application stores XML data files in the **/var/tmp/jboss/debug** directory for debugging purposes. Service request deployment, service functional audits, and any reported deployment errors from the devices are captured and stored in these XML data files.

MySQL Database Log Files

You use the MySQL database log files to view information related to the Junos Space Network Management Platform database.

Table 203 lists the MySQL database log files.

Table 203: MySQL Database Log Files

Log File	Description
/var/log/mysqld.log	Primary log file for MySQL-related procedures
var/lib/mysql/log-slow-queries.log	Log file for slow queries

Node Management Agent Log Files

A Node Management Agent (NMA) is a daemon that runs on every Junos Space node. An NMA manages the configuration files for the software components of Junos Space Network Management Platform—JBoss, MySQL, and Apache. An NMA also monitors the usage of system resources, such as CPU, memory, and disk space, and the health of the other server processes.

Table 204 lists the NMA log files.

Table 204: NMA Log Files

Log File	Description
/var/log/nma.log	Logs that contain information about operations executed on the NMA
/var/log/httpd/error_log	Error logs from NMA CGI scripts
/var/log/watchdog	Logs related to starting and stopping processes on Junos Space Network Management Platform
/var/log/SystemStatusLog	Logs related to CPU, memory, and disk space usage by Junos Space Network Management Platform

RELATED DOCUMENTATION

Troubleshooting Log File Overview | 1595

Troubleshooting Log File Overview

The troubleshooting log file is a **zip** or **tar** package that contains the log files generated by different software components of Junos Space Network Management Platform and service provisioning data files.

You can download the troubleshooting log file from the Junos Space user interface in sever mode, by accessing the Junos Space Appliance URL in maintenance mode, or from the Junos Space Appliance console in CLI mode. The troubleshooting log file is downloaded as a zip package in server mode and maintenance mode, and as a tar package in CLI mode.

- Server mode (See "Downloading the Troubleshooting Log File in Server Mode" on page 1417.)
- Maintenance mode (See "Downloading the Troubleshooting Log File in Maintenance Mode" on page 1420.)
- CLI mode (See "Downloading Troubleshooting System Log Files Through the Junos Space CLI" on page 1421.)

You need to be assigned the system administrator role to download the troubleshooting log file in server mode and maintenance mode.

Junos Space Network Management Platform automatically names the troubleshooting zip package in the **troubleshoot_*yyyy-mm-dd_hh-mm-ss*.zip** format. The date and time is represented in the Coordinated Universal Time (UTC) format. For example, **troubleshoot_2010-04-01_11-25-12.zip**.

Table 205 lists the files in this zip package.

Table 205: List of Log Files in the Troubleshooting Log File

Description	Location
JBoss log files	**/var/log/jboss/***
Service provisioning data files	**/var/tmp/jboss/debug/***
MYSQL error log file	**/var/log/mysqld.log**
Apache, NMA, and Webproxy log files	**/var/log/httpd/***
Watchdog log file	**/var/log/watchdog/***
Linux system messages	**/var/log/messages/***
CPU, RAM, and disk statistics (during past 24 hours)	**/var/log/SystemStatusLog**

RELATED DOCUMENTATION

Junos Space Network Management Platform Log Files Overview | 1591
Downloading the Troubleshooting Log File in Server Mode | 1417
Downloading the Troubleshooting Log File in Maintenance Mode | 1420
Downloading Troubleshooting System Log Files Through the Junos Space CLI | 1421

Downloading the Troubleshooting Log File in Server Mode

You download the troubleshooting log file in Server mode when you want to view the contents of the troubleshooting log file and fix issues. You need to have the privileges of a System Administrator to download the troubleshooting log file.

Before you download the troubleshooting log file in Server mode:

- Ensure that you check the available disk space on the Junos Space node. The **Lack Of Space** error message is displayed if the disk space is insufficient.
- Ensure that a troubleshooting log download job you triggered earlier is not in progress. An error message is displayed if you trigger another troubleshooting log download job while a previous download job is in progress.

> **NOTE:** On a multinode setup, the troubleshooting log file is stored at the following location on the Junos Space node that completes the job: **/var/cache/jboss/space-logs**. You cannot download the troubleshooting log file if this node goes down.

To download the troubleshooting log file in Server mode:

1. On the Junos Space Network Management Platform user interface, select **Administration > Space Troubleshooting**.

   The Space Troubleshooting page is displayed.

2. Select whether to download the troubleshooting log file now or later.

   - To download the troubleshooting log file now:

     i. Click **Download**.

     The Collect Junos Space Logs Job Information dialog box is displayed.

     ii. Click **OK** in the dialog box.

     You can download the troubleshooting log file from the Job Management page.

     iii. Double-click the ID of the troubleshooting log collection job on the Job Management page.

     The Job Details dialog box is displayed.

     iv. Click the **Download** link to access the **troubleshoot_*yyyy-mm-dd_hh-mm-ss*.zip** file in your browser.

     The filename of the troubleshoot zip file includes the server Coordinated Universal Time (UTC) date and time. For example, **troubleshoot_2010-04-01_11-25-12.zip**.

     - If you are using Mozilla Firefox: In the Opening troubleshoot zip dialog box, click **Save file**, then click **OK** to save the zip file to your computer using the Firefox Downloads dialog box.
     - If you are using Internet Explorer: From the File Download page, click **Save** and select a directory on your computer where you want to save the **troubleshoot_*yyyy-mm-dd_hh-mm-ss*.zip** file.

     > **NOTE:** If the download job failed, the Job Details dialog box displays the reason the job failed.

     Table 183 lists the files included in the **troubleshoot_*yyyy-mm-dd_hh-mm-ss*.zip** file.

     Table 206: Log Files in the Troubleshooting Log File and Their Location

Log File Description	Location
System status log file	/var/log/SystemStatusLog
JBoss log files	**/var/log/jboss/***
Service provisioning data files	**/var/tmp/jboss/debug/***
MySQL error log file	**/var/log/mysqld.log**
Apache Web Server, NMA, and Web proxy log files	**/var/log/httpd/***

Table 206: Log Files in the Troubleshooting Log File and Their Location *(continued)*

Watchdog log files	**/var/log/watchdog/***
Linux system log messages	**/var/log/messages/***
CPU, RAM, or disk statistics (for the past 24 hours)	–
Heap and CPU Profiling Agent (HPROF) files	**/var/log/jboss**

- To download the troubleshooting log file later:

  i. Select the **Schedule at a later time** option button.

  ii. Enter the date in the **Date** field in the DD/MM/YYYY format.

  iii. Enter the time in the **Time** field in the hh:mm format.

  iv. Click **Download**.

  The troubleshooting log download job is triggered at the scheduled time. You can view the status of the scheduled job on the Job Management page.

  TIP: When you contact Juniper Technical Assistance Center, describe the problem you encountered and provide the **troubleshoot_*yyyy-mm-dd_hh-mm-ss*.zip** file to the JTAC representative.

3. Click **Close** to return to the Administration statistics page.

RELATED DOCUMENTATION

System Status Log File Overview | **1408**

Customizing Node System Status Log Checking | **1410**

Customizing Node Log Files to Download | **1412**

Downloading the Troubleshooting Log File in Maintenance Mode | **1420**

Downloading Troubleshooting System Log Files Through the Junos Space CLI | **1421**

Downloading the Troubleshooting Log File in Maintenance Mode

Maintenance Mode is a special mode that an administrator can use to perform system recovery or debugging tasks while all nodes in the fabric are shut down and the Web proxy is running.

The administrator can download the **troubleshoot_*yyyy-mm-dd_hh-mm-ss*.zip** file from Maintenance Mode. The troubleshoot zip file includes the server Coordinated Universal Time (UTC) date and time. For example, **troubleshoot_2010-04-01_11-25-12.zip**.

To download the troubleshooting log file in maintenance mode, perform the following steps:

1. Connect to a Junos Space Appliance in maintenance mode by using the Junos Space Appliance URL.

   For example:

   `https://<ipaddress>/maintenance`

   Where *ipaddress* is the address of the Junos Space Appliance.

   The Maintenance Mode page appears.

2. Click the **click here to log in** link. The login dialog box appears.

3. Log in to maintenance mode by using the authorized login name and password.

4. Click OK. The Maintenance Mode Actions menu appears.

5. Click **Download Troubleshooting Data and Logs**. The file download dialog box appears.

6. Click Save to download the **troubleshoot_*yyyy-mm-dd_hh-mm-ss*.zip** file to the connected computer.

7. Click **Log Out and Exit from Maintenance Mode**.

RELATED DOCUMENTATION

- Maintenance Mode Overview | **1153**
- System Status Log File Overview | **1408**
- Customizing Node System Status Log Checking | **1410**
- Customizing Node Log Files to Download | **1412**
- Downloading the Troubleshooting Log File in Server Mode | **1417**
- Downloading Troubleshooting System Log Files Through the Junos Space CLI | **1421**

Downloading Troubleshooting System Log Files Through the Junos Space CLI

IN THIS SECTION

- Downloading a System Log File by Using a USB Device | **1600**
- Downloading System Log File by Using SCP | **1602**

If a Junos Space node is Up, the administrator can log in to the Junos Space node and download system status logs for each fabric node by using the Secure Copy Protocol (SCP). If the Junos Space node is Down but you can log in to the console of a Junos Space Appliance, you can download system status logs to a USB drive.

The **Retrieve Logs** utility collects all system log files in the **/var/log** subdirectory and creates a compressed TAR file (extension ***.tgz**). For more information about the log files that are written, see "System Status Log File Overview" on page 1408.

This topic includes the following sections:

Downloading a System Log File by Using a USB Device

Using the **Retrieve Logs** > **Save to USB Device** command, the administrator can download system status logs to a connected USB device if the Junos Space node is Down and you can log in to the console.

Before you begin, ensure that the USB device is connected to the Junos Space Appliance.

1. Log in to the Junos Space Appliance using the administrator username (admin) and password.

   The Junos Space Settings Menu appears, as shown.

```
Junos Space Settings Menu

1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> (Debug) run shell

Q> Quit
R> Redraw Menu

Choice [1-6,QR]:
```

2. Type **4** at the prompt.

   The Retrieve Logs submenu appears.

```
Choice [1-6,AQR]: 4
1> Save to USB Device
2> Send Using SCP

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-2,AMR]:
```

3. Type **1**.

   The following message is displayed: **This process will retrieve the log files on all cluster members and combine them into a .tar file. Once the file is created, you can copy the files onto a USB drive. Continue? [y/n]**

4. Type **y** to continue.

   You are prompted to enter the administrator password.

5. Enter the administrator password.

The system downloads the log files from all the nodes in the fabric and combines them into a **.tar** file. After the file is created, the file is coped to the USB device and a message similar to the following is displayed: **Copying 20090827-1511-logs.tar to USB drive**.

> **NOTE:** If the USB device is not ready, the following message appears: **Log collection complete If USB key is ready, press "Y". To abort, press "N".**

6. After the files are copied, unmount the USB and eject it from the Junos Space Appliance.

Downloading System Log File by Using SCP

Using the Junos Space CLI **Retrieve Logs** > **SCP** command, the administrator can download system status logs to a specific location.

To download system status logs by using SCP, perform the following steps:

1. Log in to the Junos Space node using the administrator username (admin) and password.

   The Junos Space Settings Menu appears, as shown.

```
Junos Space Settings Menu

1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> (Debug) run shell

Q> Quit
R> Redraw Menu

Choice [1-6,QR]:
```

2. Type **4** at the prompt.

   The Retrieve Logs submenu appears.

```
Choice [1-6,AQR]: 4
1> Save to USB Device
2> Send Using SCP
```

```
A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-2,AMR]:
```

3. Type **2**.

   The following confirmation message is displayed:

   This process will retrieve the log files on all cluster members and combine them into a .tar file. Once the file is created, you will be asked for a remote scp server to transfer the file to. Continue? [y/n]

4. Type **y** to continue.

   You are prompted to enter the administrator password.

5. Enter the administrator password.

   A message indicating that the log files are being collected is displayed. The process retrieves the log files on all cluster members and combines them into a **.TAR** file. This might take a few minutes to complete.

   After this is completed, you are prompted to enter the IP address of the remote server.

6. Enter the IP address of the SCP server to which to transfer the file.

   NOTE:
   - Depending on whether the Junos Space fabric is configured with only IPv4 addresses or both IPv4 and IPv6 addresses, Junos Space Platform allows you to enter an IPv4 address or either an IPv4 or IPv6 address respectively for the SCP server.
   - The IPv4 and IPv6 addresses that you use must be valid addresses. Refer to http://www.iana.org/assignments/ipv4-address-space for the list of restricted IPv4 addresses and http://www.iana.org/assignments/ipv6-address-space for the list of restricted IPv6 addresses.

7. Enter the remote SCP user.

8. Enter the directory on the remote SCP server where the log file should be stored; for example, **/root/tmplogs**.

   The remote server information that you entered is displayed. The following is a sample:

```
Remote scp IP: 192.0.2.0
Remote scp user: root
Remote scp path: /root/tmplogs
Is this correct? [y/n]
```

9. If the SCP server information is correct, type **y**.

   If you are connecting to the SCP server for the first time, a message is displayed asking you to confirm that you want to continue. The following is a sample message:

```
The authenticity of host '192.0.2.0 (192.0.2.0)' can't be established.
RSA key fingerprint is 01:70:4c:47:9e:1e:84:fc:69:3c:65:99:6d:e6:88:87.
Are you sure you want to continue connecting (yes/no)? yes
```

   NOTE: If the SCP server information is incorrect or if you want to modify the SCP server information, type **n** at the prompt, and modify the SCP server information as explained in the preceding steps.

10. Type **y** to continue.

    You are prompted to enter the password.

11. Enter the password for the SCP server.

    If the credentials are correct, the file is transferred to the SCP server.

RELATED DOCUMENTATION

- Maintenance Mode Overview | **1153**
- System Status Log File Overview | **1408**
- Customizing Node System Status Log Checking | **1410**
- Customizing Node Log Files to Download | **1412**
- Downloading the Troubleshooting Log File in Server Mode | **1417**
- Downloading the Troubleshooting Log File in Maintenance Mode | **1420**

Customizing Node System Status Log Checking

You customize the system status checking for a fabric node to ensure that all necessary information is written to the **/var/log/SystemStatusLog** log file. You must have the privileges of a System Administrator to customize the system status checking. You customize the system status checking by modifying the fabric node Perl script in **/usr/nma/bin/writeLogCronJob**.

To customize system status checking for a fabric node, modify the **writeSystemStatusLogFile** sub-function in **writeLogCronJob** as shown:

```
sub writeSystemStatusLogFile{
 my $err = 0;
my $logfile = $_[0];
$err = system("date >> $logfile");
$err = system("df /var >> $logfile");
$err = system("top -n 1 -b | grep Cpu >> $logfile");
$err = system("top -n 1 -b | grep Mem: >> $logfile");
$err = system("top -n 1 -b | grep Swap: >> $logfile");

***<Add additional system command here that you want to print out in the
SystemStatusLog file>***

 if ($err == 0 ) {                print "write log to $logfile successfully\n";

 } else {                print "cannot write log to $logfile\n";
 }
return $err;
 }
```

RELATED DOCUMENTATION

- System Status Log File Overview | **1408**
- Customizing Node Log Files to Download | **1412**
- Downloading the Troubleshooting Log File in Server Mode | **1417**
- Downloading the Troubleshooting Log File in Maintenance Mode | **1420**
- Downloading Troubleshooting System Log Files Through the Junos Space CLI | **1421**

Customizing Node Log Files to Download

You customize the log files downloaded for a fabric node to ensure that you download all the necessary log files. You must have the privileges of a System Administrator to customize the log files. You customize the log files you want to download by modifying the Perl script in **/var/www/cgi-bin/getLogFiles**.

Modify the **getLogFiles** Perl script zip command as shown:

```
. . .
system("zip –r $logFileName /var/log/jboss/* /var/tmp/jboss/debug/ /var/log/mysqld.log
 /var/log/httpd/* /var/log/watchdog /var/log/messages /var/log/SystemStatusLog >
/dev/null");
. . .
```

RELATED DOCUMENTATION

- System Status Log File Overview | **1408**
- Customizing Node System Status Log Checking | **1410**
- Downloading the Troubleshooting Log File in Server Mode | **1417**
- Downloading the Troubleshooting Log File in Maintenance Mode | **1420**
- Downloading Troubleshooting System Log Files Through the Junos Space CLI | **1421**

CHAPTER 87

Troubleshooting Network Devices by Using Junos Space Debug Utilties

IN THIS CHAPTER

- Junos Space Debug Utilities Overview | **1607**
- Executing Device-Connection Debug Scripts | **1611**
- Executing Device Import Detail Script and Java Application | **1626**
- Executing Job Management Scripts and Java Applications | **1629**
- Executing HornetQ Scripts | **1640**

Junos Space Debug Utilities Overview

IN THIS SECTION

- Device-Connection Debug Scripts | **1608**
- Device Import Scripts and Java Applications | **1609**
- Job Management Scripts and Java Applications | **1610**
- HornetQ Scripts | **1611**

Junos Space debug utilities allow you to debug issues related to Junos Space nodes and devices managed by Junos Space Network Management Platform and view details about jobs scheduled on Junos Space Network Management Platform. Junos Space debug utilities are a collection of scripts and Java applications stored at **/var/log/space-debug/debug-utilities**. These scripts and Java applications are organized under the following categories: deviceConnection, jobManagement, deviceImport, and HornetQ. You can save the output of the scripts at a custom location. By default, the output of the scripts is stored at the location where the scripts are stored.

The following scripts and Java applications are available for debugging:

Device-Connection Debug Scripts

IN THIS SECTION

- getDeviceInfo.sh | 1608
- DeviceDebugInfoCollector.sh | 1608
- getAllDeviceInfo.sh | 1608
- cleanupEditChannel.sh | 1609

The device-connection debug scripts stored at **/var/log/space-debug/debug-utilities/deviceConnection/** fetch and display device-connection information from DeviceDataMatrix. DeviceDataMatrix is a memory data structure in the Junos Space Network Management Platform database that stores device-connection information. You can also view this information through JConsole or JMXTerm.

The following are the device-connection debug scripts:

getDeviceInfo.sh

getDeviceInfo.sh is a script to collect device-connection information for a single device. The script output displays the device ID (as stored in the Junos Space Platform database), IP address of the device, IP address of the Junos Space node to which the device is currently connected, status of the edit flag on the device, SSH control channel number, number of channels opened from the device, and details of the open channels.

DeviceDebugInfoCollector.sh

DeviceDebugInfoCollector.sh is a script to execute frequently used Junos OS debug commands on a device. When you execute this script, SSH connections are initiated to the device from the Junos Space node you specified. The script output displays the list of active management daemon (MGD) processes on the device, active SSH daemon (SSHD) processes on the device, active SSH connections to Junos Space Platform from the device, and all active SSH connections from the device. You can also view additional details about each of these processes and SSH connections.

getAllDeviceInfo.sh

getAllDeviceInfo.sh is a script to collect device-connection information about all devices that are connected to a Junos Space node. The script output displays the device ID (as stored in the Junos Space Platform database), IP address of the device, IP address of the Junos Space node to which the device is currently connected, status of the edit flag on the device, SSH control channel number, number of channels opened from the device, and details of the open channels about all devices that are connected to a Junos Space node. On a multinode setup, you can also collect this information for all Junos Space nodes.

cleanupEditChannel.sh

cleanupEditChannel.sh is a script to unlock the device configuration on the device. Junos Space Platform sets a lock when you deploy a configuration from Junos Space Platform or Junos Space applications. You use this script to unlock the device configuration if the previous deployments were erroneous and you are currently unable to deploy the configuration from Junos Space Platform. You enter the variable *false* to unlock the device configuration.

For more information about executing device-connection debug scripts, see "Executing Device-Connection Debug Scripts" on page 1611.

Device Import Scripts and Java Applications

IN THIS SECTION

- cleanupDeviceImportTables.sh | **1609**
- DB-blob-reader.jar | **1609**

The device import scripts and Java applications stored at **/var/log/space-debug/debug-utilities/deviceImport/** clear the device import tables and fetch device inventory information or device configuration in XML format.

The following are the device import scripts and Java applications:

cleanupDeviceImportTables.sh

cleanupDeviceImportTables.sh is a script to clean data from device import tables. You can execute the script to fix data errors during a device resynchronization process. You need to manually resynchronize the device with the Junos Space Platform database from the user interface after you execute the script.

DB-blob-reader.jar

DB-blob-reader.jar is a Java application to collect the device information XML or interface information XML. When you execute this application, the information from the XML is written to the **DB-blob-reader-result.txt** file. This information can be useful for debugging device resynchronization issues. You can modify the MySQL query in the **DB-blob-reader.properties** file and fetch information based on that MySQL query. You can specify the following in the **DB-blob-reader.properties** file: device ID (as stored in the Junos Space Platform database) and name of the RPC, device configuration, or interface.

For more information about executing device import scripts and Java applications, see "Executing Device Import Detail Script and Java Application" on page 1626.

Job Management Scripts and Java Applications

IN THIS SECTION

- SystemLoadViewer.sh | 1610
- getJobThreadSump.sh | 1610
- JobInfoCollector.jar | 1610

The job management scripts and Java applications stored at **/var/log/space-debug/debug-utilities/jobManagement/** fetch information about jobs executed from the Junos Space nodes. You can also view the output of the scripts through JConsole or JMXTerm.

The following are the job management scripts and Java applications:

SystemLoadViewer.sh

SystemLoadViewer.sh is a script to collect information about available memory on all Junos Space nodes and the jobs triggered on these nodes. The script output displays information such as the memory on the nodes, number of root jobs and subjobs on each of the nodes, type of job (root job or subjob), state of the job (running, queued, or stopped), name of the job, queue name of the job, the time the job was created, and the time the job was modified. The script output also displays the top five processes that consume CPU and memory when the script is executed.

getJobThreadSump.sh

getJobThreadSump.sh is a script to view the stack trace of a specific job. You can also view the script output through JConsole or JMXTerm.

JobInfoCollector.jar

JobInfoCollector.jar is a Java application to execute SQL queries and collect information about jobs. You can construct the SQL query in the **JobInfoCollector.properties** file. This file contains a default example query. The application can also display the hierarchy of a subjob (input as the parent job ID) and list of jobs that are currently unscheduled. You can also input a SQL query to obtain information about jobs.

For more information about executing job management scripts and Java applications, see “Executing Job Management Scripts and Java Applications” on page 1629.

HornetQ Scripts

IN THIS SECTION

- HornetQInfoProvider.sh | 1611
- HQMessageViewer.sh | 1611

The HornetQ scripts stored at **/var/log/space-debug/debug-utilities/hornetQ/** display the list of all JBoss queues, of messages in a specific JBoss queue, or of jobs that are to be executed by a specific JBoss queue. You can also view the script output through JConsole or JMXTerm.

The following are the HornetQ scripts:

HornetQInfoProvider.sh

HornetQInfoProvider.sh is a script to collect details about all HornetQ queues. The script output also lists details such as consumer-count, message-count, and scheduled-count.

HQMessageViewer.sh

HQMessageViewer.sh is a script to view the list of messages in a specific JBoss queue. The script output displays the job ID and job operation name. You can view the jobs that are queued to be executed by a specific JBoss queue.

For more information about executing HornetQ scripts, see "Executing HornetQ Scripts" on page 1640.

RELATED DOCUMENTATION

Junos Space Network Management Platform Log Files Overview | 1591

Monitoring Network Devices and Troubleshooting Software Issues with Junos Space Network Management Platform | 1576

Executing Device-Connection Debug Scripts

IN THIS SECTION

- Executing the Script to Collect Device-Connection Information | 1612
- Executing the Script to Collect Device Debug Information | 1614

Executing the Script to Unlock the Device Configuration | 1619
Executing the Script to Collect Node-Connection Information | 1620

You execute the device-connection debug scripts to view information about device-connection issues related to Junos Space nodes and devices connected to these nodes. Device-connection scripts are stored at the following location: **/var/log/space-debug/debug-utilities/deviceConnection**. When you execute these scripts, the output is stored as **.txt** files at the same location. You can also specify a custom path to store the output. The following sections list the steps to execute the scripts to collect information about device-connection issues.

Executing the Script to Collect Device-Connection Information

You execute the **getDeviceInfo.sh** script to collect device-connection information of a device.

To execute the script to collect device-connection information:

1. Log in to the CLI of the Junos Space node.

2. Enter the administrator username and password at the Junos Space login prompt and press Enter.

   The default username is **admin** and the default password is **abc123**.

   The Junos Space Settings Menu is displayed.

3. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   You are prompted to enter your password.

   The following is a sample output from a virtual appliance:

```
admin@10.206.41.183's password:
Last login: Mon Aug 17 06:17:58 2015 from 10.206.41.42

Welcome to the Junos Space network settings utility.

Initializing, please wait


Junos Space Settings Menu
```

```
1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> Expand VM Drive Size
7> (Debug) run shell

A> Apply changes
Q> Quit
R> Redraw Menu

Choice [1-7,AQR]: 7
```

4. Type the administrator password and press Enter.

   The shell prompt appears.

5. Type **cd /var/log/space-debug/debug-utilities/deviceConnection** at the shell prompt and press Enter.

6. (Optional) To view the list of debug scripts, type **ls** and press Enter.

   The list of device-connection debug scripts is displayed.

7. Type **./getDeviceInfo.sh<*device-IP address*>** and press Enter—for example, **./getDeviceInfo.sh 10.206.33.17**.

   The output of this command is saved to the **DeviceInfo-<*device-IP address*>.txt** file in the same directory.

   The following is a sample output:

```
------------------------------------------------------------
Time of execution: Wed Jul 15 05:45:26 UTC 2015
------------------------------------------------------------
Device Id: 131153 Device Ip: 10.206.33.17
Node id: 10.206.41.57
Connection state: Connected
Connection changed at: 07/14/2015 17:35:04
EditFlag : false
EditChannel num:0
SSH ctrl channel num: 4
Max channels allowed: 32
Number of channels opened: 4
------------------------------------------------------
```

```
Channel details:
Channel Id: 1
Seq num: 11
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
-------------------------------------------------------
Channel Id: 2
Seq num: 14
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
-------------------------------------------------------
Channel Id: 3
Seq num: 22
Channel state: CHANNEL_STATE_OPEN
Channel type: Syslog
-------------------------------------------------------
Channel Id: 4
Seq num: 24
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
-------------------------------------------------------
```

8. (Optional) To save node connection information at a custom output location, type **./getDeviceInfo.sh<*device-IP address*> <*output-file-path*>** and press Enter.

You can use the information from the **.txt** file to debug device-connection issues.

Executing the Script to Collect Device Debug Information

You execute the **DeviceDebugInfoCollector.sh** script to collect information about the connections and processes on a device.

To execute the script to collect device debug information:

1. Log in to the CLI of the Junos Space node.

2. Enter the administrator username and password at the Junos Space login prompt and press Enter.

   The default username is **admin** and the default password is **abc123**.

   The Junos Space Settings Menu is displayed.

3. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

You are prompted to enter your password.

4. Type the administrator password and press Enter.

   The shell prompt appears.

5. Type **cd /var/log/space-debug/debug-utilities/deviceConnection** at the shell prompt and press Enter.

6. (Optional) To view the list of debug scripts, type **ls**.

   The list of device-connection debug scripts is displayed.

7. Type **./DeviceDebugInfoCollector.sh<*device-IP address*><*device-username*><*node-VIP address*>** and press Enter—for example, **./DeviceDebugInfoCollector.sh 10.206.32.107 user1 10.206.41.57**..

8. Enter the device password.

   The output from this command is saved to the **DeviceDebugInfo-<*device-IP address*>.txt** file in the same directory.

   The following is a sample output:

```
Time of execution: Wed Jul 15 07:43:43 UTC 2015
================================================================================
List of MGD processes on the device : (Command Executed - ps auxwww | sed -n
"1p; /sed -n/d; /mgd/p;")
================================================================================
USER       PID %CPU %MEM   VSZ   RSS  TT  STAT STARTED      TIME COMMAND
user1      1841  0.0  0.0 41132   236  ??  S    Fri12AM   0:10.15 /usr/sbin/mgd
 -N
user1      2310  0.0  0.0 41180   220  ??  S    Fri12AM   0:06.62 mgd: (mgd)
(user1) (mgd)
user1      2367  0.0  0.0 41180   220  ??  S    Fri12AM   0:06.67 mgd: (mgd)
(user1) (mgd)
user1      2424  0.0  0.0 41188   220  ??  S    Fri12AM   0:06.54 mgd: (mgd)
(keybased) (mgd)
user1      4243  0.0  0.1 41180   520  ??  S    12:27AM   0:02.90 mgd: (mgd)
(user1) (mgd)
user1      7662  0.0  0.1 41180   520  ??  S     2:29AM   0:02.84 mgd: (mgd)
(user1) (mgd)
user1      8595  0.0  0.2 41192  1664  ??  Is    4:09AM   0:00.07 mgd: (mgd)
(user1)/dev/ttyp2 (mgd)
user1      9065  0.0  0.0 41192   136  ??  Is    4:39AM   0:00.05 mgd: (mgd)
(user1)/dev/ttyp1 (mgd)
user1     10295  0.0  0.1 41180   520  ??  S     6:12AM   0:02.67 mgd: (mgd)
```

```
(user1) (mgd)
user1     11557  0.0  0.1 41180   520  ??  S     8:03AM   0:02.66 mgd: (mgd)
(user1) (mgd)
user1     15817  0.0  0.1 41180   520  ??  S     3:26PM   0:02.34 mgd: (mgd)
(user1) (mgd)
user1     18495  0.0  0.1 41180   520  ??  S     8:16PM   0:02.13 mgd: (mgd)
(user1) (mgd)
user1     18549  0.0  0.1 41180   520  ??  S     8:20PM   0:02.13 mgd: (mgd)
(user1) (mgd)
user1     18907  0.0  0.1 41180   520  ??  S     8:22PM   0:02.14 mgd: (mgd)
(user1) (mgd)
user1     19574  0.0  3.3 41180 25220  ??  S     8:38PM   0:02.11 mgd: (mgd)
(user1) (mgd)
user1     20290  0.0  0.6 41172  4876  ??  Is    9:46PM   0:00.10 mgd: (mgd)
(user1)/dev/ttyp0 (mgd)
user1     20794  0.0  3.3 41180 25228  ??  S     9:52PM   0:02.06 mgd: (mgd)
(user1) (mgd)
user1     21861  0.0  0.0 41180   220  ??  S    Fri09PM   0:05.93 mgd: (mgd)
(user1) (mgd)
user1     50416  0.0  0.1 41180   520  ??  S    Sun08AM   0:04.53 mgd: (mgd)
(user1) (mgd)
user1     63963  0.0  0.1 41180   520  ??  S    Sun08PM   0:04.06 mgd: (mgd)
(user1) (mgd)
user1     84282  0.0  0.1 41180   520  ??  S    Mon10AM   0:03.55 mgd: (mgd)
(user1) (mgd)
```

```
================================================================================
List of active sshd processes on the device : (Command Executed - ps auxwww |
sed -n "1p; /sed -n/d; /sshd/p;")
================================================================================
USER       PID %CPU %MEM   VSZ   RSS  TT  STAT STARTED      TIME COMMAND
user1    20972  1.7  0.4  7684  2916  ??  Ss   10:11PM   0:00.15 sshd:
user1@notty (sshd)
user1     1944  0.0  0.1  7784   692  ??  Ss   Fri12AM   1:00.95 sshd:
user1@notty (sshd)
user1     2354  0.0  0.1  7816   700  ??  Ss   Fri12AM   1:00.21 sshd:
user1@notty (sshd)
user1     2378  0.0  0.1  7820   700  ??  Ss   Fri12AM   1:00.39 sshd:
keybased@notty (sshd)
user1     3907  0.0  0.1  7784   772  ??  Ss   12:27AM   0:10.47 sshd:
user1@notty (sshd)
user1     5334  0.0  0.0  7676   320  ??  Is    1:25AM   0:00.30 sshd:
user1@ttyp1 (sshd)
user1     5361  0.0  0.1  7676   476  ??  Is    1:26AM   0:00.25 sshd:
user1@ttyp2 (sshd)
```

```
user1      7649  0.0  0.1  7784   776  ??  Ss    2:29AM   0:07.62 sshd:
user1@notty (sshd)
user1     10284  0.0  0.1  7784   468  ??  Ss    6:11AM   0:02.11 sshd:
user1@notty (sshd)
user1     11544  0.0  0.1  7784   776  ??  Ss    8:03AM   0:04.69 sshd:
user1@notty (sshd)
user1     15806  0.0  0.1  7784   788  ??  Ss    3:26PM   0:03.38 sshd:
user1@notty (sshd)
user1     18484  0.0  0.1  7784   792  ??  Ss    8:16PM   0:02.99 sshd:
user1@notty (sshd)
user1     18538  0.0  0.1  7784   776  ??  Ss    8:20PM   0:03.47 sshd:
user1@notty (sshd)
user1     18896  0.0  0.1  7796   784  ??  Ss    8:22PM   0:02.89 sshd:
user1@notty (sshd)
user1     19561  0.0  0.4  7784  2924  ??  Ss    8:38PM   0:02.41 sshd:
user1@notty (sshd)
user1     20272  0.0  0.4  7684  2900  ??  Is    9:46PM   0:00.26 sshd:
user1@ttyp0 (sshd)
user1     20783  0.0  0.4  7796  2932  ??  Ss    9:52PM   0:00.52 sshd:
user1@notty (sshd)
user1     21820  0.0  0.1  7800   696  ??  S    Fri09PM   0:47.90 sshd:
user1@notty (sshd)
user1     50401  0.0  0.1  7784   776  ??  Ss   Sun08AM   0:36.25 sshd:
user1@notty (sshd)
user1     63919  0.0  0.1  7796   784  ??  Ss   Sun08PM   0:34.21 sshd:
user1@notty (sshd)
user1     84233  0.0  0.1  7784   776  ??  Ss   Mon10AM   0:20.37 sshd:
user1@notty (sshd)
================================================================================
List of open SSH connections to 10.206.41.57 from  the device : (Command Executed
 -  netstat -tln | egrep "Pro|\.7804"; netstat -tln | grep "\.22"). Please note
 that of the listed connections, one is opened by this debug script to collect
 the debug information from the device
================================================================================
Proto Recv-Q Send-Q  Local Address                                  Foreign
Address                                (state)
tcp4       0      0  10.206.32.107.22
10.206.41.57.43098                             ESTABLISHED
tcp4       0      0  10.206.32.107.22
10.206.41.57.33080                             ESTABLISHED
================================================================================
List of open SSH connections on the device : (Command Executed - netstat -tln
| egrep "Pro|\.7804"; netstat -tln grep "\.22")
================================================================================
```

```
Proto Recv-Q Send-Q  Local Address                                Foreign
Address                                (state)
tcp4       0      0  10.206.32.107.58052
10.206.41.46.7804                                SYN_SENT
tcp4       0      0  10.206.32.107.53398
10.206.41.192.7804                               ESTABLISHED
tcp4       0      0  10.206.32.107.22
10.206.41.57.43098                               ESTABLISHED
tcp4       0      0  10.206.32.107.22
10.206.41.62.60026                               ESTABLISHED
tcp4       0      0  10.206.32.107.22
10.206.155.85.62406                              ESTABLISHED
tcp4       0      0  10.206.32.107.22
10.206.41.143.39926                              ESTABLISHED
tcp4       0      0  10.206.32.107.22
10.207.70.104.36730                              ESTABLISHED
tcp4       0      0  10.206.32.107.22
10.206.41.171.52993                              ESTABLISHED
tcp4       0      0  10.206.32.107.22
10.206.41.33.45765                               ESTABLISHED
tcp4       0      0  10.206.32.107.22
10.206.41.211.50000                              ESTABLISHED
tcp4       0      0  10.206.32.107.22
10.206.41.57.33080                               ESTABLISHED
tcp4       0      0  10.206.32.107.22
10.206.41.156.49032                              ESTABLISHED
tcp4       0      0  10.206.32.107.22
10.206.40.4.38068                                ESTABLISHED
tcp4       0      0  10.206.32.107.22
10.206.41.240.61583                              ESTABLISHED
tcp4       0      0  10.206.32.107.22
10.206.41.240.61569                              ESTABLISHED
tcp4       0      0  10.206.32.107.22
10.206.41.149.60804                              ESTABLISHED
tcp4       0      0  10.206.32.107.22
10.206.41.235.59358                              ESTABLISHED
tcp4       0      0  10.206.32.107.22
10.206.41.231.34530                              ESTABLISHED
tcp4       0      0  10.206.32.107.22
10.206.41.221.48186                              ESTABLISHED
tcp4       0      0  10.206.32.107.22
10.205.56.82.41163                               ESTABLISHED
tcp4       0      0  10.206.32.107.22
10.161.11.161.42174                              ESTABLISHED
```

```
tcp4       0      0  10.206.32.107.22
10.206.41.71.47831                         ESTABLISHED
```

9. (Optional) To save device debug connection information at a custom output location, type **./DeviceDebugInfoCollector.sh*<device-IP address>* *<device-username>* *<node-VIP address>* *<output-file-path>*** and press Enter..

You can use the information from the **.txt** file to debug issues related to the connections and processes on the device.

Executing the Script to Unlock the Device Configuration

You execute the **cleanupEditChannel.sh** script to unlock the device configuration.

To execute the script to unlock the device configuration:

1. Log in to the CLI of the Junos Space node.

2. Enter the administrator username and password at the Junos Space login prompt and press Enter.

   The default username is **admin** and the default password is **abc123**.

   The Junos Space Settings Menu is displayed.

3. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   You are prompted to enter your password.

4. Type the administrator password and press Enter.

   The shell prompt appears.

5. Type **cd /var/log/space-debug/debug-utilities/deviceConnection** at the shell prompt and press Enter.

6. (Optional) To view the list of debug scripts, type **ls** and press Enter.

   The list of device-connection debug scripts is displayed.

7. Type **./cleanupEditChannel.sh *<device-IP address>*false** and press Enter—for example, **./cleanupEditChannel.sh 10.206.33.17 false**.

   You can modify the configuration on the device from the Junos Space user interface.

Executing the Script to Collect Node-Connection Information

You execute the **getAllDeviceInfo.sh** script to collect information about devices connected to a Junos Space node. You can also execute the script to collect information about devices connected to all the nodes in your Junos Space setup.

To execute the script to collect node-connection information:

1. Log in to the CLI of the Junos Space node.

2. Enter the administrator username and password at the Junos Space login prompt and press Enter.

   The default username is **admin** and the default password is **abc123**.

   The Junos Space Settings Menu is displayed.

3. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   You are prompted to enter your password.

4. Type the administrator password and press Enter.

   The shell prompt appears.

5. Type **cd /var/log/space-debug/debug-utilities/deviceConnection** at the shell prompt and press Enter.

6. (Optional) To view the list of debug scripts, type **ls** and press Enter.

7. Type **./getAllDeviceInfo.sh <*node-VIP address*>** and press Enter—for example, **./getAllDeviceInfo.sh 10.206.41.57**.

   The output from this command is saved to the **DeviceInfoOutput.txt** file in the same directory.

   The following is a sample output:

```
------------------------------------------------------------
Time of execution: Wed Jul 15 05:35:21 UTC 2015
------------------------------------------------------------
Device Id: 131129 Device Ip: 10.206.32.107
Node id: 10.206.41.57
Connection state: Connected
Connection changed at: 07/14/2015 17:35:04
EditFlag : false
EditChannel num:0
SSH ctrl channel num: 6
```

```
Max channels allowed: 32
Number of channels opened: 6
-----------------------------------------------------
Channel details:
Channel Id: 1
Seq num: 10
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
-----------------------------------------------------
Channel Id: 2
Seq num: 16
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
-----------------------------------------------------
Channel Id: 3
Seq num: 21
Channel state: CHANNEL_STATE_OPEN
Channel type: Syslog
-----------------------------------------------------
Channel Id: 4
Seq num: 23
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
-----------------------------------------------------
Channel Id: 5
Seq num: 110
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
-----------------------------------------------------
Channel Id: 6
Seq num: 112
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
-----------------------------------------------------
=====================================================
Device Id: 131153 Device Ip: 10.206.33.17
Node id: 10.206.41.57
Connection state: Connected
Connection changed at: 07/14/2015 17:35:04
EditFlag : false
EditChannel num:0
SSH ctrl channel num: 4
Max channels allowed: 32
Number of channels opened: 4
```

```
-----------------------------------------------------
Channel details:
Channel Id: 1
Seq num: 11
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
-----------------------------------------------------
Channel Id: 2
Seq num: 14
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
-----------------------------------------------------
Channel Id: 3
Seq num: 22
Channel state: CHANNEL_STATE_OPEN
Channel type: Syslog
-----------------------------------------------------
Channel Id: 4
Seq num: 24
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
-----------------------------------------------------
=====================================================
Device Id: 131233 Device Ip: 127.0.0.1
Node id: 10.206.41.57
Connection state: Connected
Connection changed at: 07/14/2015 17:35:17
EditFlag : false
EditChannel num:0
SSH ctrl channel num: 13
Max channels allowed: 32
Number of channels opened: 7
-----------------------------------------------------
Channel details:
Channel Id: 1
Seq num: 26
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
-----------------------------------------------------
Channel Id: 2
Seq num: 27
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
-----------------------------------------------------
```

```
Channel Id: 3
Seq num: 28
Channel state: CHANNEL_STATE_OPEN
Channel type: Syslog
------------------------------------------------------
Channel Id: 4
Seq num: 102
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
------------------------------------------------------
Channel Id: 5
Seq num: 103
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
------------------------------------------------------
Channel Id: 6
Seq num: 113
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
------------------------------------------------------
Channel Id: 7
Seq num: 114
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
------------------------------------------------------
======================================================
Device Id: 131149 Device Ip: 10.206.40.1
Node id: 10.206.41.57
Connection state: Connected
Connection changed at: 07/14/2015 17:35:03
EditFlag : false
EditChannel num:0
SSH ctrl channel num: 5
Max channels allowed: 32
Number of channels opened: 5
------------------------------------------------------
Channel details:
Channel Id: 1
Seq num: 9
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
------------------------------------------------------
Channel Id: 2
Seq num: 15
```

```
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
------------------------------------------------------
Channel Id: 3
Seq num: 20
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
------------------------------------------------------
Channel Id: 4
Seq num: 25
Channel state: CHANNEL_STATE_OPEN
Channel type: Syslog
------------------------------------------------------
Channel Id: 5
Seq num: 29
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
------------------------------------------------------
======================================================
Device Id: 131121 Device Ip: 10.206.32.186
Node id: 10.206.41.57
Connection state: Connected
Connection changed at: 07/14/2015 17:35:03
EditFlag : false
EditChannel num:0
SSH ctrl channel num: 3
Max channels allowed: 32
Number of channels opened: 6
------------------------------------------------------
Channel details:
Channel Id: 1
Seq num: 8
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
------------------------------------------------------
Channel Id: 2
Seq num: 17
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
------------------------------------------------------
Channel Id: 3
Seq num: 18
Channel state: CHANNEL_STATE_OPEN
Channel type: Syslog
```

```
-------------------------------------------------------
Channel Id: 4
Seq num: 19
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
-------------------------------------------------------
Channel Id: 5
Seq num: 109
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
-------------------------------------------------------
Channel Id: 6
Seq num: 111
Channel state: CHANNEL_STATE_UNUSE
Channel type: Netconf
-------------------------------------------------------
=======================================================
```

8. (Optional) To save node connection information at a custom output location, type **./getAllDeviceInfo.sh *<node-VIP address>* *<output-file-path>*** and press Enter.

9. (Optional) To view connection information across all nodes, type **./getAllDeviceInfo.sh ALL-NODES** and press Enter.

You can use the information from the **.txt** file to debug issues related to devices connected to a single or multiple Junos Space nodes.

RELATED DOCUMENTATION

Junos Space Debug Utilities Overview | **1607**

Monitoring Network Devices and Troubleshooting Software Issues with Junos Space Network Management Platform | **1576**

Executing Device Import Detail Script and Java Application

IN THIS SECTION

- Executing the Script to Delete Data from Device Import Tables | 1626
- Executing the Java Application to View Device XML | 1627

You execute the device import script to delete data from device import tables. You execute the **DB-blob-reader.jar** Java application to view device information in XML format. Device import script and Java application are stored at the following location: **/var/log/space-debug/debug-utilities/deviceImport**. When you execute the Java application, the output is stored as a **.txt** file at the same location. The following sections list the steps to execute the script to delete device import details and Java application to view device information.

Executing the Script to Delete Data from Device Import Tables

You execute the **cleanupDeviceImportTables.sh** script to delete data from device import tables.

To execute the script to delete data from device import tables:

1. Log in to the CLI of the Junos Space node.

2. Enter the administrator username and password at the Junos Space login prompt and press Enter.

   The default username is **admin** and the default password is **abc123**.

   The Junos Space Settings Menu is displayed.

3. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   You are prompted to enter your password.

   The following is a sample output from a virtual appliance:

   ```
   admin@10.206.41.183's password:
   Last login: Mon Aug 17 06:17:58 2015 from 10.206.41.42

   Welcome to the Junos Space network settings utility.

   Initializing, please wait
   ```

```
Junos Space Settings Menu

1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> Expand VM Drive Size
7> (Debug) run shell

A> Apply changes
Q> Quit
R> Redraw Menu

Choice [1-7,AQR]: 7
```

4. Type the administrator password and press Enter.

   The shell prompt appears.

5. Type **cd /var/log/space-debug/debug-utilities/deviceImport** at the shell prompt and press Enter.

6. (Optional) To view the list of device import scripts and Java applications, type **ls** and press Enter.

7. Type **./cleanupDeviceImportTables.sh *<database-username>* *<database-password>* *<database-name>* *<device-name>*** and press Enter. For example:

```
./cleanupDeviceImportTables.sh jboss netscreen build_db ABC123
Warning: Using a password on the command line interface can be insecure.
Device id from ABC123 is :XXXXX
Warning: Using a password on the command line interface can be insecure.
Finished cleaning up the import related tables for device ABC123
```

Executing the Java Application to View Device XML

You execute the **DB-blob-reader.jar** application to view the device XML information.

Ensure that you have updated the MySQL query in the **DB-blob-reader.properties** file before executing the Java application. The file also contains an example configuration.

To execute the Java application and view a device XML:

1. Log in to the CLI of the Junos Space node.

2. Enter the administrator username and password at the Junos Space login prompt and press Enter.

   The default username is **admin** and the default password is **abc123**.

   The Junos Space Settings Menu is displayed.

3. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   You are prompted to enter your password.

4. Type the administrator password and press Enter.

   The shell prompt appears.

5. Type **cd /var/log/space-debug/debug-utilities/deviceImport** at the shell prompt and press Enter.

6. (Optional) To view the list of device import scripts and Java applications, type **ls** and press Enter.

7. Type **/usr/bin/java -jar DB-blob-reader.jar** and press Enter.

8. Enter the database username.

9. Enter the database password.

   The output from this command is saved to the **DB-blob-reader-result.txt** file in the same directory.

You can view the output of the query you entered in the **DB-blob-reader.properties** file.

RELATED DOCUMENTATION

Junos Space Debug Utilities Overview | **1607**

Monitoring Network Devices and Troubleshooting Software Issues with Junos Space Network Management Platform | **1576**

Executing Job Management Scripts and Java Applications

IN THIS SECTION

- Executing the Java Application to Collect Job Information | 1629
- Executing the Script to View the Stack Trace of a Job | 1633
- Executing the Script to View Job Information on Nodes | 1634

You execute job management scripts and Java applications to view information about jobs triggered from Junos Space nodes. The JobInfoCollector.jar Java application and the job management scripts are stored at the following location: **/var/log/space-debug/debug-utilities/jobManagement**. When you execute the JobInfoCollector.jar Java application and job management scripts, the output is stored as **.txt** files at the same location. You can also specify a custom path to store the output. The following sections list the steps to execute the scripts to collect information about jobs.

Executing the Java Application to Collect Job Information

You execute the JobInfoCollector.jar application to collect job information. Ensure that you have updated the MySQL query in the **JobInfoCollector.properties** file before executing the Java application. The file also contains an example configuration.

To execute the Java application to collect job information:

1. Log in to the CLI of the Junos Space node.

2. Enter the administrator username and password at the Junos Space login prompt and press Enter.

   The default username is **admin** and the default password is **abc123**.

   The Junos Space Settings Menu is displayed.

3. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   You are prompted to enter your password.

   The following is a sample output from a virtual appliance:

   ```
   admin@10.206.41.183's password:
   Last login: Mon Aug 17 06:17:58 2015 from 10.206.41.42
   ```

```
Welcome to the Junos Space network settings utility.

Initializing, please wait


Junos Space Settings Menu

1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> Expand VM Drive Size
7> (Debug) run shell

A> Apply changes
Q> Quit
R> Redraw Menu

Choice [1-7,AQR]: 7
```

4. Type the administrator password and press Enter.

   The shell prompt appears.

5. Type **cd /var/log/space-debug/debug-utilities/jobManagement** at the shell prompt and press Enter.

6. (Optional) To view the list of job management scripts and Java applications, enter **ls** and press Enter.

7. Type **/usr/bin/java -jar JobInfoCollector.jar** and press Enter.

   The following options will be displayed:

```
Please select an option from below:
1. Display job parent-children hierarchy
2. Filter from job data
3. Display jobs not yet picked up by Job Dispatcher
```

8. Type **1**, **2**, or **3** to select an option.

9. Enter the database username.

10. Enter the database password.

11. The inputs displayed depend on the option you selected.

    If you selected option 1, you need to enter the parent job ID.

    - Enter a job ID.

      The output from this command is saved to the **JobHierarchy-<*job-ID*>.txt** file in the same directory. The following is a sample output if you selected 1:

```
=====Job details for 491529 =====

NODE: 10.206.41.57
STARTTIMESTAMP: 17 Jul 2015 17:51:00 GMT
JOBSTATE: Done
JOBSTATUS: Success
ENDTIMESTAMP: 17 Jul 2015 17:52:15 GMT
CHILDCOUNT: 2

 Child job details:

ID || NODE || STARTTIMESTAMP || JOBSTATE || JOBSTATUS || ENDTIMESTAMP ||
CHILDCOUNT ||
 491530 | 10.206.41.57 | 17 Jul 2015 17:51:01 GMT | Done | Success | 17 Jul
2015 17:51:13 GMT | 0 |
 491531 | 10.206.41.57 | 17 Jul 2015 17:51:01 GMT | Done | Success | 17 Jul
2015 17:51:13 GMT | 0 |
```

    If you selected option 2, you need to enter a MySQL query.

- Enter a MySQL query—for example, **mostate='Failure'**.

  This query filters the jobs that failed. The following is a sample output if you selected 2:

```
ID || NAME || NODE || STARTTIMESTAMP || JOBSTATE || JOBSTATUS || ENDTIMESTAMP
 ||
 196608 | Discover Network Elements-196608 | 10.206.41.184 | 10 Aug 2015
10:44:48 GMT | Done | Failure | 10 Aug 2015 10:48:47 GMT |
 196624 | Discover Network Elements-196624 | 10.206.41.184 | 10 Aug 2015
10:49:52 GMT | Done | Failure | 10 Aug 2015 10:49:58 GMT |
 196643 | Mail User Password-196643 | 10.206.41.184 | 10 Aug 2015 14:11:21
GMT | Done | Failure | 10 Aug 2015 14:11:21 GMT |
 196649 | Mail User Password-196649 | 10.206.41.184 | 11 Aug 2015 02:39:18
GMT | Done | Failure | 11 Aug 2015 02:39:18 GMT |
 196650 | Mail User Password-196650 | 10.206.41.184 | 11 Aug 2015 02:39:18
GMT | Done | Failure | 11 Aug 2015 02:39:18 GMT |
 196660 | Sync Files-196660 | 10.206.41.187 | 11 Aug 2015 11:54:13 GMT | Done
 | Failure | 11 Aug 2015 11:54:46 GMT |
 360448 | Resync Network Elements-360448 | 10.206.41.184 | 11 Aug 2015 18:06:07
 GMT | Done | Failure | 11 Aug 2015 18:06:08 GMT |
 360449 | Discover Network Elements-360449 | 10.206.41.187 | 11 Aug 2015
18:12:43 GMT | Done | Failure | 11 Aug 2015 18:13:16 GMT |
```

If you selected option 3, the list of unscheduled jobs is saved to the **UnscheduledJobs.txt** file in the same directory.

- The following is a sample output if you selected 3:

```
ID || NAME || JOBSTATE || PARENTJOBID ||
 393501 | ND Discovery-393501 | Done | 0 |
 393858 | Backup Configuration Files-393858 | Done | 0 |
 720906 | ND Discovery-720906 | Done | 0 |
 721067 | Backup Configuration Files-721067 | Done | 0 |
 721884 | Backup Configuration Files-721884 | Done | 0 |
 1048659 | Backup Configuration Files-1048659 | Done | 0 |
 1182260 | Enable Script-1182260 | InProgress | 0 |
 1182413 | Execute Script-1182413 | InProgress | 0 |
 1183914 | Backup Configuration Files-1183914 | Done | 0 |
 1184310 | Delete Device-1184310 | Done | 0 |
 1189992 | Stage Script-1189992 | InProgress | 0 |
 1190105 | Update Network Element-1190105 | InProgress | 0 |
 1442231 | Backup Configuration Files-1442231 | Done | 0 |
 1442232 | -1442232 | InProgress | 1184310 |
 1442233 | -1442233 | InProgress | 1184310 |
 1442234 | -1442234 | InProgress | 1184310 |
 1442235 | -1442235 | InProgress | 1184310 |
 1442236 | -1442236 | InProgress | 1184310 |
 1442237 | -1442237 | InProgress | 1184310 |
 1442238 | -1442238 | InProgress | 1184310 |
 1442239 | -1442239 | InProgress | 1184310 |
 1442240 | -1442240 | InProgress | 1184310 |
 1445400 | Generate SD LR Report-1445400 | Scheduled | 0 |
 1445528 | Cloud Infrastructure Event Purge-1445528 | Scheduled | 0 |
 1445602 | Policy Hits Collection-1445602 | Scheduled | 0 |
 1903749 | useraccounts-1903749 | Done | 0 |
```

You can view the hierarchy of a subjob (input as the parent job ID), list of jobs that are currently unscheduled, or the output based on the query you entered in the **JobInfoCollector.properties** file.

Executing the Script to View the Stack Trace of a Job

You execute the **getJobThreadDump.sh** script to view the stack trace of a job.

To execute the script to view the stack trace of a job:

1. Log in to the CLI of the Junos Space node.

2. Enter the administrator username and password at the Junos Space login prompt and press Enter.

   The default username is **admin** and the default password is **abc123**.

The Junos Space Settings Menu is displayed.

3. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   You are prompted to enter your password.

4. Type the administrator password and press Enter.

   The shell prompt appears.

5. Type **cd /var/log/space-debug/debug-utilities/jobManagement** at the shell prompt and press Enter.

6. (Optional) To view the list of job management scripts and Java applications, type **ls** and press Enter.

7. Type **./getJobThreadDump.sh <*job-ID*>** and press Enter.

   The output from this command is saved to the **JobThreadDump-<*job-ID*>.txt** file in the same directory.

8. (Optional) To save the stack trace of the job at a custom output location, type **./getJobThreadDump.sh <*job-ID*> <*output-file-path*>** and press Enter.

Executing the Script to View Job Information on Nodes

You execute the **SystemLoadViewer.sh** script to view job information on a node.

To execute the script to view job information on a node:

1. Log in to the CLI of the Junos Space node.

2. Enter the administrator username and password at the Junos Space login prompt and press Enter.

   The default username is **admin** and the default password is **abc123**.

   The Junos Space Settings Menu is displayed.

3. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   You are prompted to enter your password.

4. Type the administrator password and press Enter.

   The shell prompt appears.

5. Type **cd /var/log/space-debug/debug-utilities/jobManagement** at the shell prompt and press Enter.

6. (Optional) To view the list of job management scripts and Java applications, type **ls** and press Enter.

7. Type **./SystemLoadViewer.sh** and press Enter.

   The output from this command is saved to the **./SystemLoadInfo.txt** file in the same directory. The following is a sample output from the command:

```
------------------------------------------------------------
Time of execution: Mon Jul 20 06:54:14 UTC 2015
------------------------------------------------------------

====================NODE SUMMARY=====================
Node IP: 10.206.41.35
Maximum JVM memory: 2040528896
Estimated memory usage per node: 40465
Reserved memory size: 20000000
(Available Memory = Maximum JVM memor - Estimated memory usage per node - Reserved
 memory)
Available Memory:2020488431
Number of first root jobs on this node:1
Number of next root jobs on this node:0
Number of sub jobs on this node:0
-----------------------------------------
=========================================
Node load statistics:
=========================================
Resource Id:autoresync-group:132832:user1@host:03604710000000000008G
Type:autoresync-group
SubType:132832
Context type:FIRST_ROOT_JOB
State:RUNNING
Queue:
Node IP:10.206.41.35
Creation Time:2015-07-20 06:54:13.166
Last modification time:2015-07-20 06:54:13.166
Estimated Memory:40465
=========================================
============================SYSTEM LOAD SUMMARY FOR LOCAL
NODE============================
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/mapper/jmpvgnocf-lvvar
                      52772604   2584204  47373632   6% /var
======Command executed: LINES=20 COLUMNS=120 top -n 2 -b -c | tail -n
+22=================
top - 06:54:18 up 3 days, 19:01,  2 users,  load average: 1.24, 0.88, 0.82
```

```
Tasks: 271 total,   2 running, 268 sleeping,   0 stopped,   1 zombie
Cpu(s): 42.2%us, 23.5%sy,  0.5%ni, 32.7%id,  0.3%wa,  0.1%hi,  0.7%si,  0.0%st
Mem:   7937672k total,  7827836k used,   109836k free,   539116k buffers
Swap:  8193140k total,   132684k used,  8060456k free,  1246572k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
30383 user1      20   0 83616  24m 2508 S 36.8  0.3   0:02.16 /usr/bin/perl
/var/www/cgi-bin/secure/resourceMonitoring
 4204 jboss     20   0 4081m 2.7g  14m S 27.6 36.0 395:59.73
/usr/lib/jvm/java-1.7.0-openjdk-1.7.0.79.x86_64/jre/bin/jav
31240 user1      20   0  124m  15m 2448 S  7.6  0.2   0:00.23 perl -e use
lib("/usr/nma/lib"); use NmaUtil; print NmaUtil
31251 user1      20   0 72016  14m 2384 R  6.9  0.2   0:00.21 perl -e use
lib("/usr/nma/lib"); use NmaDb; print NmaDb::ge
30719 mysql     16  -4 2936m 744m 6628 S  3.6  9.6  62:17.79 /usr/sbin/mysqld
--basedir=/usr --datadir=/var/lib/mysql --
32329 opennms   25   5 3446m 877m  21m S  3.0 11.3 164:35.59
/usr/lib/jvm/jre-1.7.0-openjdk.x86_64/bin/java -Djava.endor
 3120 user1      20   0 84612  21m 2460 S  1.0  0.3  13:51.23 /usr/bin/perl
/usr/bin/jmp-sync
30651 user1      20   0 12896 1436  952 R  1.0  0.0   0:00.07 top -n 2 -b -c
13332 user1      20   0  154m 9824 4480 S  0.7  0.1  26:56.92 /usr/sbin/snmpd
-Lsd -Lf /dev/null -p /var/run/snmpd.pid -a
18186 postgres  20   0  268m  12m 9252 S  0.7  0.2   0:00.38 postgres: opennms
 opennms 127.0.0.1(55330) idle
 2589 jboss     20   0  924m 197m  10m S  0.3  2.5   6:11.24 java -D[Host
Controller] -Dorg.jboss.boot.log.file=/var/log
15335 apache    23   3  141m 4936 3012 S  0.3  0.1   0:00.62 /usr/sbin/httpd
======Command executed: COLUMNS=120 top -n 1 -b -c | egrep
'(mysqld|java|postgres)'========
 4204 jboss     20   0 4081m 2.7g  14m S  1.9 36.0 395:59.74
/usr/lib/jvm/java-1.7.0-openjdk-1.7.0.79.x86_64/jre/bin/jav
32329 opennms   25   5 3446m 877m  21m S  1.9 11.3 164:35.60
/usr/lib/jvm/jre-1.7.0-openjdk.x86_64/bin/java -Djava.endor
 2556 jboss     20   0  527m  47m 9800 S  0.0  0.6   4:44.43 java -D[Process
Controller] -server -Xms32m -Xmx128m -XX:Ma
 2589 jboss     20   0  924m 197m  10m S  0.0  2.5   6:11.24 java -D[Host
Controller] -Dorg.jboss.boot.log.file=/var/log
 2886 postgres  20   0  268m  10m 7524 S  0.0  0.1   0:00.10 postgres: opennms
 opennms 127.0.0.1(55289) idle
 2888 postgres  20   0  268m  10m 7580 S  0.0  0.1   0:00.08 postgres: opennms
 opennms 127.0.0.1(55290) idle
 2889 postgres  20   0  268m  10m 8040 S  0.0  0.1   0:00.15 postgres: opennms
 opennms 127.0.0.1(55291) idle
```

```
 2891 postgres  20   0  268m  12m 9352 S  0.0  0.2   0:00.31 postgres: opennms
 opennms 127.0.0.1(55292) idle
 2893 postgres  20   0  267m  10m 7612 S  0.0  0.1   0:00.09 postgres: opennms
 opennms 127.0.0.1(55293) idle
 2895 postgres  20   0  267m 8968 6548 S  0.0  0.1   0:00.03 postgres: opennms
 opennms 127.0.0.1(55294) idle
 3507 jboss     20   0  528m  47m 9856 S  0.0  0.6   4:51.80 java -D[Process
Controller] -server -Xms32m -Xmx128m -XX:Ma
 3561 jboss     20   0  566m 143m  10m S  0.0  1.8   5:43.77 java -D[Host
Controller] -Dorg.jboss.boot.log.file=/var/log
 5570 postgres  20   0  266m 4680 2784 S  0.0  0.1   0:00.01 postgres: opennms
 opennms 127.0.0.1(36280) idle
 5572 postgres  20   0  266m 4688 2792 S  0.0  0.1   0:00.01 postgres: opennms
 opennms 127.0.0.1(36281) idle
 5573 postgres  20   0  266m 4676 2780 S  0.0  0.1   0:00.01 postgres: opennms
 opennms 127.0.0.1(36282) idle
 5575 postgres  20   0  266m 4684 2788 S  0.0  0.1   0:00.01 postgres: opennms
 opennms 127.0.0.1(36283) idle
 5578 postgres  20   0  266m 4696 2800 S  0.0  0.1   0:00.00 postgres: opennms
 opennms 127.0.0.1(36284) idle
 5579 postgres  20   0  266m 4688 2792 S  0.0  0.1   0:00.01 postgres: opennms
 opennms 127.0.0.1(36285) idle
 5581 postgres  20   0  266m 4680 2784 S  0.0  0.1   0:00.00 postgres: opennms
 opennms 127.0.0.1(36286) idle
 5583 postgres  20   0  266m 4676 2780 S  0.0  0.1   0:00.01 postgres: opennms
 opennms 127.0.0.1(36287) idle
 5586 postgres  20   0  266m 4680 2784 S  0.0  0.1   0:00.00 postgres: opennms
 opennms 127.0.0.1(36288) idle
 5587 postgres  20   0  266m 4676 2780 S  0.0  0.1   0:00.01 postgres: opennms
 opennms 127.0.0.1(36289) idle
 5590 postgres  20   0  266m 4692 2796 S  0.0  0.1   0:00.00 postgres: opennms
 opennms 127.0.0.1(36290) idle
 5591 postgres  20   0  266m 4692 2796 S  0.0  0.1   0:00.00 postgres: opennms
 opennms 127.0.0.1(36291) idle
 5593 postgres  20   0  266m 4696 2800 S  0.0  0.1   0:00.00 postgres: opennms
 opennms 127.0.0.1(36292) idle
 5595 postgres  20   0  266m 4680 2784 S  0.0  0.1   0:00.00 postgres: opennms
 opennms 127.0.0.1(36293) idle
 5597 postgres  20   0  266m 4676 2780 S  0.0  0.1   0:00.01 postgres: opennms
 opennms 127.0.0.1(36294) idle
 5599 postgres  20   0  266m 4684 2788 S  0.0  0.1   0:00.00 postgres: opennms
 opennms 127.0.0.1(36295) idle
 5601 postgres  20   0  268m  10m 8172 S  0.0  0.1   0:00.14 postgres: opennms
 opennms 127.0.0.1(36296) idle
```

```
 5603 postgres  20   0  268m  10m 7376 S  0.0  0.1   0:00.07 postgres: opennms
 opennms 127.0.0.1(36297) idle
 5605 postgres  20   0  267m 9.8m 7228 S  0.0  0.1   0:00.05 postgres: opennms
 opennms 127.0.0.1(36298) idle
 5607 postgres  20   0  267m 9972 7132 S  0.0  0.1   0:00.06 postgres: opennms
 opennms 127.0.0.1(36299) idle
 5609 postgres  20   0  268m  10m 8252 S  0.0  0.1   0:00.20 postgres: opennms
 opennms 127.0.0.1(36300) idle
 5611 postgres  20   0  268m  11m 8848 S  0.0  0.2   0:00.21 postgres: opennms
 opennms 127.0.0.1(36301) idle
 8123 postgres  20   0  268m  10m 8160 S  0.0  0.1   0:00.14 postgres: opennms
 opennms 127.0.0.1(56849) idle
17000 user1      20   0 2299m  68m 8072 S  0.0  0.9   6:32.60 ./jre/bin/java
-Djava.compiler=NONE -cp /usr/StorMan/RaidMa
18186 postgres  20   0  268m  12m 9256 S  0.0  0.2   0:00.38 postgres: opennms
 opennms 127.0.0.1(55330) idle
18187 postgres  20   0  268m  11m 8800 S  0.0  0.2   0:00.18 postgres: opennms
 opennms 127.0.0.1(55331) idle
18188 postgres  20   0  268m  10m 7484 S  0.0  0.1   0:00.09 postgres: opennms
 opennms 127.0.0.1(55332) idle
18190 postgres  20   0  268m  10m 7800 S  0.0  0.1   0:00.10 postgres: opennms
 opennms 127.0.0.1(55333) idle
20287 postgres  20   0  266m 4680 2784 S  0.0  0.1   0:00.00 postgres: opennms
 opennms 127.0.0.1(36339) idle
20289 postgres  20   0  266m 4676 2780 S  0.0  0.1   0:00.00 postgres: opennms
 opennms 127.0.0.1(36340) idle
20291 postgres  20   0  266m 4684 2788 S  0.0  0.1   0:00.00 postgres: opennms
 opennms 127.0.0.1(36341) idle
20297 postgres  20   0  266m 4680 2784 S  0.0  0.1   0:00.00 postgres: opennms
 opennms 127.0.0.1(36342) idle
20298 postgres  20   0  266m 4676 2780 S  0.0  0.1   0:00.00 postgres: opennms
 opennms 127.0.0.1(36343) idle
20301 postgres  20   0  267m 7448 5228 S  0.0  0.1   0:00.01 postgres: opennms
 opennms 127.0.0.1(36344) idle
20306 postgres  20   0  267m 7804 5548 S  0.0  0.1   0:00.01 postgres: opennms
 opennms 127.0.0.1(36345) idle
20308 postgres  20   0  267m 9660 6872 S  0.0  0.1   0:00.06 postgres: opennms
 opennms 127.0.0.1(36346) idle
20311 postgres  20   0  268m  10m 7692 S  0.0  0.1   0:00.14 postgres: opennms
 opennms 127.0.0.1(36347) idle
22848 postgres  20   0  266m 4684 2788 S  0.0  0.1   0:00.00 postgres: opennms
 opennms 127.0.0.1(56892) idle
22850 postgres  20   0  266m 4680 2784 S  0.0  0.1   0:00.01 postgres: opennms
 opennms 127.0.0.1(56893) idle
```

```
22852 postgres  20   0  266m 4676 2780 S  0.0  0.1   0:00.00 postgres: opennms
 opennms 127.0.0.1(56894) idle
22858 postgres  20   0  266m 6388 4312 S  0.0  0.1   0:00.01 postgres: opennms
 opennms 127.0.0.1(56895) idle
22860 postgres  20   0  268m  10m 7452 S  0.0  0.1   0:00.11 postgres: opennms
 opennms 127.0.0.1(56896) idle
22863 postgres  20   0  268m  10m 7968 S  0.0  0.1   0:00.22 postgres: opennms
 opennms 127.0.0.1(56897) idle
22864 postgres  20   0  267m 7608 5368 S  0.0  0.1   0:00.02 postgres: opennms
 opennms 127.0.0.1(56898) idle
22866 postgres  20   0  268m  10m 7528 S  0.0  0.1   0:00.13 postgres: opennms
 opennms 127.0.0.1(56899) idle
29715 user1      16  -4 13052 1068 1064 S  0.0  0.0   0:00.11 /bin/sh
/usr/bin/mysqld_safe --datadir=/var/lib/mysql --pid
30719 mysql     16  -4 2936m 744m 6628 S  0.0  9.6  62:17.79 /usr/sbin/mysqld
--basedir=/usr --datadir=/var/lib/mysql --
31064 postgres  20   0  265m  17m  16m S  0.0  0.2   0:32.35
/usr/pgsql-9.4/bin/postmaster -p 5432 -D /var/lib/pgsql/9.4
31072 postgres  20   0  119m 1728  868 S  0.0  0.0   0:03.28 postgres: logger
process
31074 postgres  20   0  265m  42m  41m S  0.0  0.5   0:39.87 postgres:
checkpointer process
31075 postgres  20   0  265m 7304 6368 S  0.0  0.1   0:05.45 postgres: writer
process
31076 postgres  20   0  265m 6076 5156 S  0.0  0.1   0:53.84 postgres: wal writer
 process
31077 postgres  20   0  265m 2688 1496 S  0.0  0.0   0:12.46 postgres: autovacuum
 launcher process
31078 postgres  20   0  119m 2056  924 S  0.0  0.0   0:58.40 postgres: stats
collector process
31304 user1      20   0 61220  768  664 S  0.0  0.0   0:00.00 egrep
(mysqld|java|postgres)
```

8. (Optional) To save job information about a node at a custom output location, enter **./SystemLoadViewer.sh <*output-file-path*>**.

You can view information such as the memory on the nodes, number of root jobs and subjobs on each of the nodes, and so on.

RELATED DOCUMENTATION

Junos Space Debug Utilities Overview | 1607

Monitoring Network Devices and Troubleshooting Software Issues with Junos Space Network Management Platform | 1576

Executing HornetQ Scripts

IN THIS SECTION

- Executing the HornetQ Script to View all JBoss Queues | 1640
- Executing the HornetQ Script to List of Messages in a JBoss Queue | 1642

You execute HornetQ scripts to fetch details about all queues from the JBoss CLI or view the list of messages on a specific queue. HornetQ scripts are stored at the following location: **/var/log/space-debug/debug-utilities/HornetQ**. When you execute these scripts, the output is stored as **.txt** files at the same location. You can also specify a custom path to store the output. The following sections list the steps to execute the scripts to fetch details about queues from the JBoss CLI.

Executing the HornetQ Script to View all JBoss Queues

You execute the **HornetQInfoProvider.sh** script to view all the JBoss queues.

To execute the script to view all JBoss queues:

1. Log in to the CLI of the Junos Space node.

2. Enter the administrator username and password at the Junos Space login prompt and press Enter.

   The default username is **admin** and the default password is **abc123**.

   The Junos Space Settings Menu is displayed.

3. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   You are prompted to enter your password.

   The following is a sample output from a virtual appliance:

   ```
   admin@10.206.41.183's password:
   Last login: Mon Aug 17 06:17:58 2015 from 10.206.41.42
   ```

```
Welcome to the Junos Space network settings utility.

Initializing, please wait


Junos Space Settings Menu

1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> Expand VM Drive Size
7> (Debug) run shell

A> Apply changes
Q> Quit
R> Redraw Menu

Choice [1-7,AQR]: 7
```

4. Type the administrator password and press Enter.

   The shell prompt appears.

5. Type **cd /var/log/space-debug/debug-utilities/hornetQ** at the shell prompt and press Enter.

6. (Optional) To view the list of HornetQ scripts, type **ls** and press Enter.

7. Type **./HornetQInfoProvider.sh** and press Enter.

   The output from this command is saved to the **HornetQInfo.txt** file in the same directory. The following sample output displays one of the JBoss queues:

```
------------------------------------------------------------
Time of execution: Tue Jul 21 05:58:23 UTC 2015
------------------------------------------------------------
==============================10.206.41.57==============================
 {
    "outcome" => "success",
    "result" => [
{
```

```
            "address" => [
                ("subsystem" => "messaging"),
                ("hornetq-server" => "default"),
                ("jms-queue" => "timeOutQueue")
            ],
            "outcome" => "success",
            "result" => {
                "consumer-count" => 15,
                "dead-letter-address" => "jms.queue.DLQ",
                "delivering-count" => 0,
                "durable" => true,
                "entries" => ["queue/timeOutQueue"],
                "expiry-address" => undefined,
                "message-count" => 0L,
                "messages-added" => 0L,
                "paused" => false,
                "queue-address" => "jms.queue.timeOutQueue",
                "scheduled-count" => 0L,
                "selector" => undefined,
                "temporary" => false
            }
        },
```

8. (Optional) To save the list of all JBoss queues at a custom output location, type **./getDeviceInfo.sh<*output-file-path*>** and press Enter.

You can view all the JBoss queues.

Executing the HornetQ Script to List of Messages in a JBoss Queue

You execute the **HornetQInfoProvider.sh** script to view the list of messages in a JBoss queue.

To execute the script to view the list of messages in a JBoss queue:

1. Log in to the CLI of the Junos Space node.

2. Enter the administrator username and password at the Junos Space login prompt and press Enter.

   The default username is **admin** and the default password is **abc123**.

   The Junos Space Settings Menu is displayed.

3. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

You are prompted to enter your password.

The following is a sample output from a virtual appliance:

```
admin@10.206.41.183's password:
Last login: Mon Aug 17 06:17:58 2015 from 10.206.41.42

Welcome to the Junos Space network settings utility.

Initializing, please wait


Junos Space Settings Menu

1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> Expand VM Drive Size
7> (Debug) run shell

A> Apply changes
Q> Quit
R> Redraw Menu

Choice [1-7,AQR]: 7
```

4. Type the administrator password and press Enter.

   The shell prompt appears.

5. Type **cd /var/log/space-debug/debug-utilities/hornetQ** at the shell prompt and press Enter.

6. (Optional) To view the list of HornetQ scripts, type **ls** and press Enter.

7. Type **./HornetQMessageViewer.sh*<queue-name>***—for example, **./HornetQMessageViewer.sh*ResyncJobDispatcherQueue***.

   The output from this command is saved to the ***<queue-name>*-messages.txt** file in the same directory. The following sample output displays the list of messages in a JBoss queue named ResyncJobDispatcherQueue.

```
------------------------------------------------------------
Time of execution: Tue Jun  2 16:13:51 PDT 2015
------------------------------------------------------------
[{"consumerName":"ServerConsumer [id=0, filter=null, binding=LocalQueueBinding
 [address=jms.queue.ResyncJobDispatcherQueue,
queue=QueueImpl[name=jms.queue.ResyncJobDispatcherQueue, postOffice=PostOfficeImpl

[server=HornetQServerImpl::serverUUID=d2f96781-0972-11e5-9e84-69e3a4c4a918]]@3ead3529]]",
"elements":[{"timestamp":1433286830611,
"userID":"ID:0780c666-097d-11e5-9e84-69e3a4c4a918",
"messageID":37172,
"JobOperationName":"executeResyncDevices",
"expiration":0,
"address":"jms.queue.ResyncJobDispatcherQueue",
"priority":4,
"JobId":196669,
"__HQ_CID":"077f8de2-097d-11e5-9e84-69e3a4c4a918",
"durable":false,"type":2}]}]
```

8. (Optional) To save the list of all messages at a custom output location, type **./HornetQMessageViewer.sh<*queue-name*> <*output-file-path*>** and press Enter.

You can view the list of messages in a specific JBoss queue.

RELATED DOCUMENTATION

Junos Space Debug Utilities Overview | **1607**

Monitoring Network Devices and Troubleshooting Software Issues with Junos Space Network Management Platform | **1576**

PART 15

Troubleshooting Junos Space Platform Issues

Troubleshooting Login–Related Issues | **1646**

Troubleshooting Device Management–Related Issues | **1648**

Troubleshooting Network Monitoring–Related Issues | **1651**

Troubleshooting DMI Schema–Related Issues | **1652**

CHAPTER 88

Troubleshooting Login–Related Issues

IN THIS CHAPTER

- Troubleshooting the Not Able to Log In from the Junos Space Login Page Issue | 1646

Troubleshooting the Not Able to Log In from the Junos Space Login Page Issue

Problem

Description: You cannot login to Junos Space Network Management Platform from the Junos Space login page. The login page displays a message stating the possible cause of the issue.

Cause

You may not be able to log in from the Junos Space login page for one of the following reasons:

- You entered an incorrect username, password, or both.

  The following message is displayed on the login page: The username or password is incorrect
- Your account is locked because you exceeded the maximum number of login attempts

  The following message is displayed on the login page: The account is Locked. You can't Log in

  NOTE: By default, your account is locked out after four unsuccessful login attempts.

Solution

- If you have entered incorrect login credentials, verify and enter the correct login credentials.
- If your account is locked

  1. Try logging in from another system.
  2. Contact the administrator to unlock your user account.

NOTE: Your user account is automatically unlocked in 24 hours.

RELATED DOCUMENTATION

Troubleshooting Device Discovery Failure | 1648

CHAPTER 89

Troubleshooting Device Management–Related Issues

IN THIS CHAPTER

- Troubleshooting Device Discovery Failure | 1648
- Troubleshooting Device Data Collection Issue | 1649
- Troubleshooting Devices Discovered Twice Using the Device Discovery Workflow | 1650

Troubleshooting Device Discovery Failure

Problem

Description: Devices are not discovered to Junos Space Network Management Platform.

Symptoms: The devices you tried to discover to Junos Space Network Management Platform are not listed on the Device Management page.

The device discovery job for devices discovered through a device discovery profile, listed on the Job Management page fails.

Cause

You cannot discover devices to Junos Space Network Management Platform for one of the following reasons:

- You provided an incorrect password to access the device through the Device Discovery Profile workflow.
- You provided an incorrect private key or passphrase during the Device Discovery Profile workflow
- The device is not reachable.
- You provided incorrect SNMP settings for the device in the Device Discovery workflow.

Solution

- If you entered an incorrect password, modify the device discovery profile by reentering the password and rediscover the device by using the Device Discovery Profile workflow.
- If you uploaded an incorrect private key or passphrase, modify the device discovery profile by uploading the correct private key and passphrase and rediscover the device by using the Device Discovery Profile workflow.

- If the device you are trying to discover is not reachable, add the correct route to the device. For more information about adding a route to the device, refer to the appropriate device configuration guide.
- If you entered incorrect SNMP settings for the device, you can do one of the following:
  - Modify the device discovery profile by clearing the **Use SNMP** check box on the **Network Management Platform > Devices > Device Discovery Profiles > Modify Device Discovery Profile > Specify Probes** page and rediscover the device.
  - Modify the device discovery profile by adding the correct SNMP details on the **Network Management Platform > Devices > Device Discovery Profiles > Modify Device Discovery Profile > Specify Probes** page and rediscover the device.

> **NOTE:** Ensure that SNMP is enabled on the device. For more information about enabling SNMP on the device, refer to the appropriate device configuration guide.

RELATED DOCUMENTATION

Troubleshooting Device Data Collection Issue | 1649

Troubleshooting Device Data Collection Issue

Problem

Description: The device on Junos Space Network Management Platform displays the Managed status but the device is not able to collect data.

Cause

A device cannot collect data even though the status of the device is Managed for one of the following reasons:

- You have not updated the SNMP settings of the device. You may have chosen to skip updating the SNMP details when you discovered the device to Junos Space Network Management Platform.
- You have not selected the device interfaces for data collection.

Solution

- If you have not updated the SNMP settings of the device, update the SNMP settings on the **Network Management Platform > Network Monitoring > Admin** page.
- If you have not selected the device interfaces for data collection:

1. Select the device on the **Network Management Platform > Network Monitoring > Admin > Configure SNMP Data Collection per Interface** page.
2. In the Collect column, select **Collect** or **Default** from the drop-down list corresponding to the interfaces.

RELATED DOCUMENTATION

Troubleshooting Device Discovery Failure | 1648

Troubleshooting Devices Discovered Twice Using the Device Discovery Workflow

Problem

Description: Using the Device Discovery Profile workflow, devices are discovered twice to Junos Space Network Management Platform.

Cause

You are using the ping-only method to discover devices to Junos Space Network Management Platform.

Solution

Select the SNMP check box on the **Network Management Platform > Devices > Device Discovery Profile > Create Device Discovery Profile > Specify Probes** when discovering devices using the Device Discovery Profile workflow. Enabling the SNMP option ensures that Junos Space Network Management Platform checks the serial number of the devices during the discovery process. This prevents the discovery process from adding duplicate instances of the devices to Junos Space Network Management Platform.

RELATED DOCUMENTATION

Troubleshooting Device Discovery Failure | 1648

CHAPTER 90

Troubleshooting Network Monitoring–Related Issues

IN THIS CHAPTER

- Troubleshooting the Network Monitoring Page Is Not Available Issue | 1651

Troubleshooting the Network Monitoring Page Is Not Available Issue

Problem

Description: You can navigate to all other workspaces but the Network Monitoring workspace is not accessible.

Cause

The Network Monitoring service has stopped unexpectedly.

Solution

Restart the Network Monitoring service. To restart the Network Monitoring service:

1. Navigate to the **Network Management .Platform > Administration > Applications** page.
2. Right-click **Network Management Platform** and select **Manage Services** from the Actions menu.
3. Select **Network Monitoring**, then select the Restart Service icon.

RELATED DOCUMENTATION

Troubleshooting Device Discovery Failure | 1648

CHAPTER 91

Troubleshooting DMI Schema–Related Issues

IN THIS CHAPTER

- Troubleshooting the Nondisplay of the DMI Schema Tree Issue | 1652

Troubleshooting the Nondisplay of the DMI Schema Tree Issue

Problem

Description: The DMI schema tree is not displayed.

Symptoms: On the Create Template Definition page, you cannot navigate the DMI schema tree or the hierarchy of configuration options on the left.

Cause

The DMI schema is defective or corrupt.

If the topmost node (Configuration) cannot be opened to reveal the hierarchy, the schema was corrupted during transition. (Use the **grep** command to search for SchemaMgr ERROR in the **server.log** file.)

> **NOTE:** One defective schema does not affect other schemas, which are still available for use.

Solution

Use your own compressed TAR file. This does not require you to restart JBoss. Ensure that the **Enable Schema Overwrite** check box is selected when you update the schema. For instructions to add or update a DMI schema , see "Adding Missing DMI Schemas or Updating Outdated DMI Schemas by Using the Update Schema Menu" on page 1548 in the *Junos Space Network Management Platform Workspaces User Guide*.

For instructions to create your own compressed TAR file, see "Creating a Compressed TAR File for Updating DMI Schema" on page 1553 in the *Junos Space Network Management Platform Workspaces User Guide*.

RELATED DOCUMENTATION

Monitoring Network Devices and Troubleshooting Software Issues with Junos Space Network Management Platform | **1576**

High Availability and Disaster Recovery Guide

PART 16

High Availability

Overview | **1656**

Understanding the High Availability Software Architecture | **1659**

Understanding the Junos Space Cluster (Fabric) Architecture | **1666**

Configuring High Availability Overview | **1681**

High Availability Failover Scenarios | **1687**

CHAPTER 92

Overview

IN THIS CHAPTER

- Junos Space High Availability Overview | 1656
- High Availability Characteristics of Junos Space Appliances | 1658

Junos Space High Availability Overview

Junos Space is designed as a carrier-grade system that provides a complete fault tolerant solution. The set of topics describing Junos Space high availability (HA) provide an overview of the Junos Space high availability design and implementation, as well as all the steps that are required to deploy a high availability solution, from ordering your appliances and preparing a Junos Space high availability cluster, to final deployment.

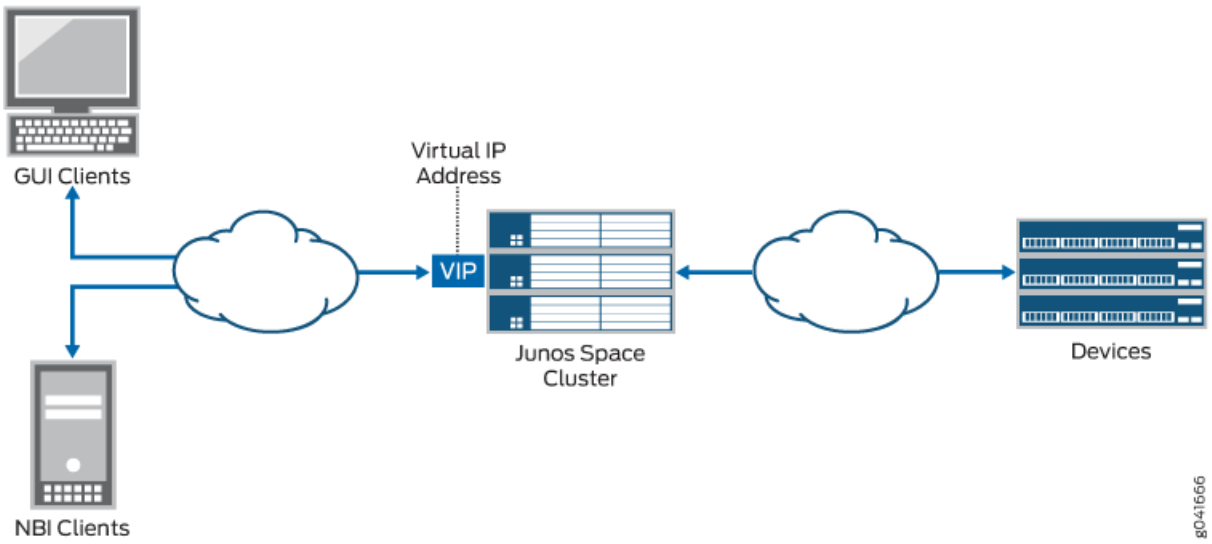
In order to gain an understanding of the Junos Space high availability solution, we recommend that you read all the Junos Space high availability topics. However, if you are primarily interested in setting up high availability, including the prerequisite steps, see the "Configuring the Junos Space Cluster for High Availability Overview" on page 1681 topic. If you are interested in high availability for network monitoring, see "High Availability for Network Monitoring" on page 1677. A set of frequently asked questions about Junos Space high availability are also answered in FAQ: Junos Space High Availability.

Junos Space Network Management Platform is available in two form factors:

- JA2500 carrier-grade hardware appliance
- Virtual appliance for the VMware ESX server or Kernel-based Virtual Machine (KVM) environment

Both the Junos Space hardware appliance and virtual appliance use the same software build with identical features to provide the complete package including OS, databases, load balancers and JBoss engines. You can cluster multiple appliances together to form a Junos Space cluster, as shown in Figure 145.

Figure 145: Deployment of a Junos Space Cluster



A Junos Space fabric (cluster) can contain only hardware appliances (JA2500), only virtual appliances, or a combination of both hardware and virtual appliances. Each appliance in the cluster is called a *node*. Junos Space cluster architecture also incorporates load balancing across all nodes in the cluster, which becomes the basis for providing scalability for a Junos Space deployment.

A Junos Space high availability solution comprises the following key components:

- Junos Space cluster architecture allows multiple Junos Space appliances (hardware or virtual) to be connected together to form a single cluster. All services within the cluster are provided through a single virtual IP address that GUI and Northbound Interface (NBI) clients can use. This architecture provides protection against any single point of failure (SPOF) in the cluster. If any node in the cluster fails, all services continue to be available, albeit with reduced capacity.

  Four logical clusters can be formed within the single physical cluster when Junos Space appliances are connected together. For more information, see "Understanding the Logical Clusters Within a Junos Space Cluster" on page 1666.

- The Junos Space Appliance (JA2500) is a carrier-grade hardware appliance designed to ensure hardware-level reliability and incorporates several fault tolerance features to eliminate single point of failure and minimize its downtime. The Junos Space Appliance contributes significantly to the availability of the overall cluster. For more information, see the "High Availability Characteristics of Junos Space Appliances" on page 1658 topic.

- The Watchdog service provides process-level high availability. In the event of any software services failure on a Junos Space appliance, the watchdog service automatically restarts the service.

RELATED DOCUMENTATION

Junos Space High Availability Software Architecture Overview | 1659

High Availability Characteristics of Junos Space Appliances

Junos Space Appliances (JA2500) incorporate the following fault tolerance features that prevent or minimize their downtime and contribute significantly to the availability of the overall cluster:

- Hot-swappable hard disk drives managed by a RAID controller
  - The hot-swappable hard drives on Junos Space appliances are externally accessible in field-replaceable trays, providing component high availability. You can remove and replace a hard disk without powering off the appliance or disrupting any functions performed by the appliance.
  - The RAID controller manages the hard disk drives and presents them as logical units.
- Option to install a redundant power supply module—Junos Space Appliances are shipped with a single AC power supply. However, you can install an additional power supply module that serves as a redundant power supply if one power supply module fails. If you install a second power supply module, ensure that you plug in each power supply module into a separate power circuit.

  When an appliance has an additional redundant, functioning power supply module that is plugged into a separate power circuit, the power supply modules are hot-swappable.
- Two cooling fans—Two externally accessible and hot-swappable cooling fans provide the required airflow and cooling for the appliance.

For detailed information about Junos Space Appliances, refer to the *Hardware Documentation* section of the *Junos Space and Applications* page.

RELATED DOCUMENTATION

Junos Space High Availability Overview | 1656

CHAPTER 93

Understanding the High Availability Software Architecture

IN THIS CHAPTER

- Junos Space High Availability Software Architecture Overview | 1659
- Software Components for Junos Space Nodes | 1663

Junos Space High Availability Software Architecture Overview

IN THIS SECTION

- Junos Space Software Architecture | 1660
- Load-Balancing Architecture | 1661
- Database Architecture | 1661
- Inter-Node Communication Among Nodes in a Junos Space Cluster | 1662

The Junos Space platform is designed to ensure five-nines availability with a clustered, multi-tiered, distributed architecture comprising the following features:

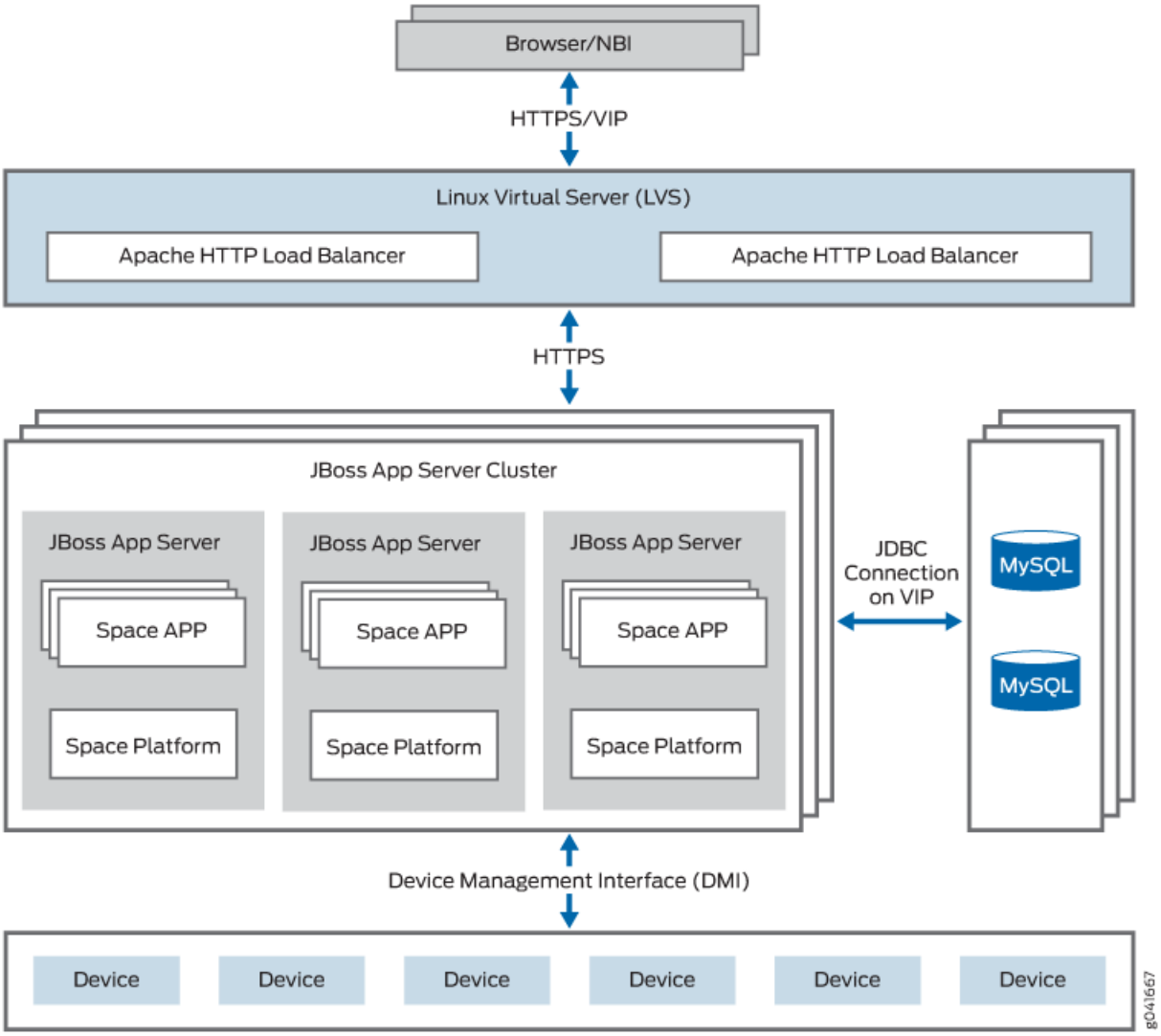
- Standard browser-based Web 2.0 GUI clients and REST/HTTPS-based NBI clients
- Apache Load Balancer as a top-level load balancer
- JBoss Application Server based on J2EE technology to provide application framework
- MySQL database to manage persistent data
- Cassandra distributed file system to store device image files and files from Junos Space applications

The following sections describe the Junos Space architecture and identify the basic requirements for communication between nodes in a Junos Space cluster:

Junos Space Software Architecture

Figure 146 provides a high-level view of the Junos Space software architecture. Junos Space services are accessible to GUI and NBI clients by means of a single virtual IP address for the cluster.

Figure 146: Junos Space Software Architecture



The requests from clients are load-balanced between multiple nodes in the cluster through the Apache HTTP Load Balancer, which is deployed in an active-hot standby configuration on two nodes in the cluster. The load balancer on the node which owns the virtual IP (VIP) address acts as the active instance. If the node which currently owns the VIP address goes down, the other node in the Linux Virtual Server (LVS) cluster will detect this failure and automatically take over the VIP address. The HTTP requests are load-balanced across all active JBoss servers in the cluster using a round-robin algorithm.

Active JBoss servers within the cluster provide the application framework for Junos Space applications, including the following services:

- Hosting the applications and associated business logic
- Application-level load balancing within the cluster
- Application monitoring and automatic recovery
- Cluster node monitoring and automatic recovery
- Database services with direct access to MySQL DB through JDBC
- Hosting Device Mediation Logic

Load-Balancing Architecture

A Junos Space cluster is presented with two kinds of loads:

- Incoming requests from GUI and NBI clients
- Communication with managed devices

Junos Space is designed to load-balance incoming requests across all active nodes in the cluster. Requests from GUI and NBI clients arrive as HTTP requests serviced by the active instance of the Apache HTTP load balancer. The load balancer distributes the requests to all active JBoss servers in the cluster using a round-robin algorithm. Sticky sessions are utilized to ensure that all HTTP requests associated with a specific GUI session are served by the same JBoss server during the lifetime of that session. For the purpose of application-level load balancing, JBoss business logic processes complex requests as a set of sub-jobs, which are distributed across multiple nodes in the cluster. For example, a single request to a four-node Space cluster to resynchronize 100 devices is divided into four sub-jobs that are executed on four different nodes, with each node resynchronizing 25 devices. For a detailed overview of load balancing, see the topic “Understanding the Logical Clusters Within a Junos Space Cluster” on page 1666.

To perform device-level load balancing, Junos Space employs logic in the Device Mediation Layer (DML) so that device connections are equally distributed across all active nodes in the cluster. Device-level load balancing is performed during device discovery by comparing the number of device connections served by individual nodes and selecting the least loaded node. If any node goes down, all associated device connections are distributed to the remaining active nodes in the cluster, thus preventing a node outage from affecting device connectivity. For a detailed overview of device connectivity management, see the topic “Understanding High Availability Management of DMI Connections” on page 1676.

Database Architecture

MySQL Enterprise Edition is used to provide database services for managing persistent data for both platform and applications. MySQL DB servers are running on two nodes in the cluster in active-standby configuration. Database transactions are replicated between the two MySQL servers in near real-time.

For information about the MySQL cluster that is formed within each Junos Space cluster, see "Understanding the Logical Clusters Within a Junos Space Cluster" on page 1666.

Junos Space platform also incorporates network monitoring for fault and performance management, which uses the PostgreSQL relational database service for storing fault and performance related data. The PostgreSQL server runs on two nodes in the Space cluster in active-active configuration with real-time replication to ensure that fault and performance data continues to be available even if one of these nodes fail. For more information, see "High Availability for Network Monitoring" on page 1677.

Inter-Node Communication Among Nodes in a Junos Space Cluster

In order to facilitate seamless communication between the nodes in a Space cluster and to achieve optimum performance of the cluster, you need to ensure the following:

- All nodes in a Junos Space cluster are configured with IP addresses inside the same subnet. This is important for the VIP switchover mechanism to work correctly.
- All nodes in a Space cluster are connected by means of a 1-Gbps or 100-Mbps local network with negligible latency.
- JBoss servers within a Junos Space cluster communicate by means of a UDP multicast to form logical clusters.

> **NOTE:** UDP multicast traffic must be allowed within the nodes in the cluster, which also means that you should disable IGMP snooping on the switches that interconnect the cluster or configure them explicitly to allow UDP multicast between the nodes.

Release History Table

Release	Description
15.2R2	Cassandra distributed file system to store device image files and files from Junos Space applications

RELATED DOCUMENTATION

Junos Space High Availability Overview | 1656

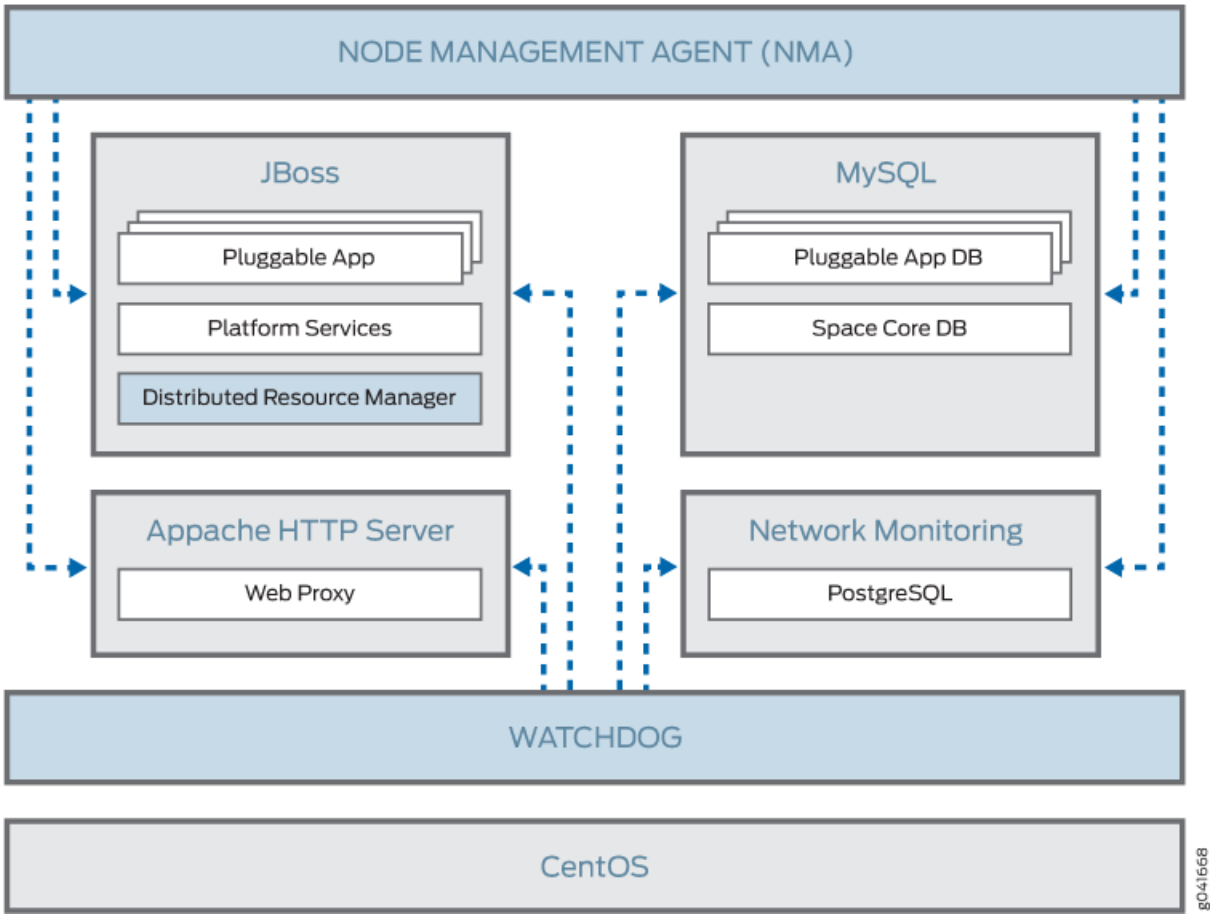
Software Components for Junos Space Nodes | 1663

Understanding the Logical Clusters Within a Junos Space Cluster | 1666

Software Components for Junos Space Nodes

The Junos Space Appliance (JA2500) and Junos Space virtual appliance both run the same software stack, as shown in Figure 147.

Figure 147: Software Stack on a Junos Space Appliance



The Junos Space software architecture is based on a combination of the following mature and proven software components:

- CentOS 6.8 distribution is used as the underlying OS of the appliance. CentOS distribution is binary compatible with Red Hat Enterprise Linux (RHEL). Services that are required for Junos Space are leveraged from this distribution, with all other services removed. Junos Space administrators do not need to directly access the Linux components because all operations, administration, and management (OAM) of the platform is performed from the Junos Space user interface or CLI. At the same time, it is important to note that the underlying operating system is an industry-standard distribution with a strong heritage of reliability and security.
- The MySQL Enterprise Edition 5.6 relational database service provides persistent storage for the Junos Space Network Management Platform and all hosted applications. A common database instance stores

all persistent data that the Network Management Platform requires. As shown in the preceding illustration, each pluggable application that is installed on the platform has its own unique database instance. All database instances are contained within a single MySQL server, which runs on two nodes in the cluster to form an active-standby cluster. The remaining nodes in the cluster do not run a MySQL server.

- JBoss 7.1 Application Server is the container that hosts the presentation layer, business logic layer, and data access layer of Junos Space platform as well as the hosted applications. One JBoss server runs on each node in the cluster and they all work together as a single load-sharing cluster.
- Apache HTTP Server (version 2.2.34) is the front-end load balancer for all requests coming from GUI and NBI clients. This server runs on two nodes in the cluster which together form an active-standby cluster.
- Network monitoring services are provided using OpenNMS, which is an award winning, enterprise-grade network monitoring platform developed under the open source model. OpenNMS is integrated into the Junos Space Network Management Platform **Network Monitoring** workspace and provides fault monitoring and performance monitoring features. Junos Space uses PostgreSQL as the relational database server for persisting fault and performance data.

The following software components or services also play a significant role in the overall management of a Junos Space cluster:

- Distributed Resource Manager (DRM)—DRM is deployed as a service inside the JBoss application server, just like all other services provided by Network Management Platform and the hosted applications. You can think of DRM as the server-side component that you interact with when you navigate to the **Network Management Platform > Administration > Fabric** workspace in the Junos Space user interface. DRM works together with the Node Management Agent to fulfill the following responsibilities:
  - Managing the Junos Space cluster—DRM implements the business logic for adding and removing nodes in the cluster and monitors the overall health of the cluster.
  - Managing the logical clusters in the cluster—The logical clusters within the physical cluster formed by the Junos Space nodes include the Apache Load Balancer cluster, JBoss cluster, and Database cluster. DRM implements the business logic to add and remove nodes in these logical clusters and monitors their status. The logical clusters are described in detail in “Understanding the Logical Clusters Within a Junos Space Cluster” on page 1666.
- Node Management Agent (NMA)—NMA runs on each node in the cluster and is deployed as a set of CGI scripts run by an Apache HTTP daemon. NMA has the following responsibilities:
  - Monitor system resource usage on the node and the health of various services running on the node.
  - Start and stop services on the node based on requests from DRM.
  - Manage the configuration files for various services running on the node.
  - Manage installation, uninstallation, and upgrades of pluggable applications as well as upgrade of the Network Management Platform software on the node.

- Watchdog—The watchdog service (jmp-watchdog) runs on each node in the cluster to ensure that required services on the node are running. Every second, the watchdog checks that the required services are running and if the watchdog detects that a service is down, it restarts the service.

RELATED DOCUMENTATION

Junos Space High Availability Overview | **1656**

Junos Space High Availability Software Architecture Overview | **1659**

Understanding the Logical Clusters Within a Junos Space Cluster | **1666**

CHAPTER 94

Understanding the Junos Space Cluster (Fabric) Architecture

IN THIS CHAPTER

- Understanding the Logical Clusters Within a Junos Space Cluster | **1666**
- Understanding Virtual IP Availability Within a Junos Space Cluster | **1673**
- Understanding High Availability Nodes in a Cluster | **1674**
- Understanding High Availability Management of DMI Connections | **1676**
- High Availability for Network Monitoring | **1677**
- Understanding How Devices Are Configured to Send SNMP Traps to Junos Space | **1679**

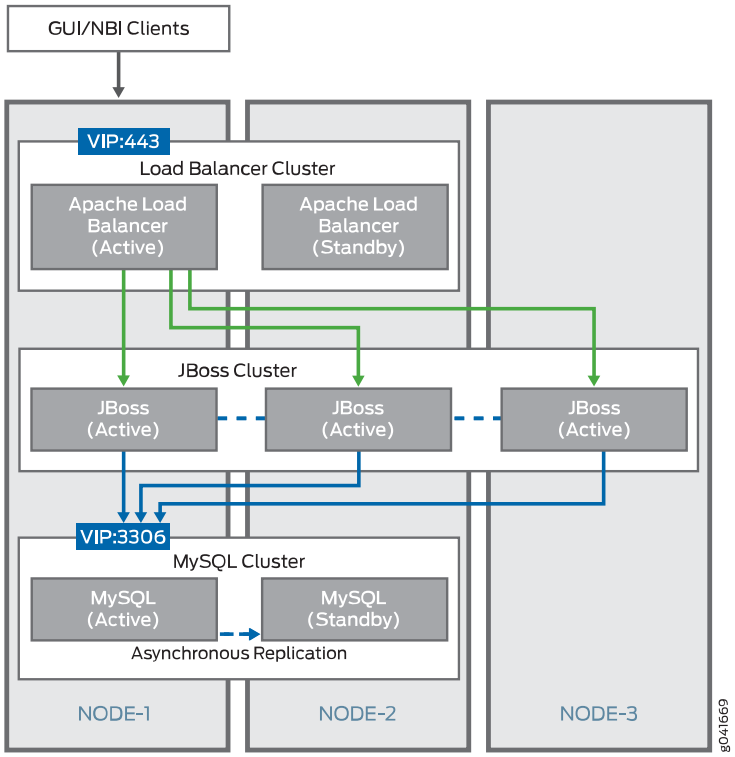
Understanding the Logical Clusters Within a Junos Space Cluster

IN THIS SECTION

- Apache Load-Balancer Cluster | **1667**
- JBoss Cluster | **1668**
- MySQL Cluster | **1669**
- Cassandra Cluster | **1671**

You can connect multiple Junos Space appliances (hardware or virtual) together to form a Junos Space cluster. Figure 148 shows the logical clusters (Apache Load Balancer cluster, the JBoss cluster, and MySQL cluster) that are formed within each Junos Space cluster.

Figure 148: Junos Space Logical Clusters



Apache Load-Balancer Cluster

The Apache HTTP server, with the mod_proxy load-balancer module enabled, runs on two nodes in the cluster at any given time. These servers form an active-standby logical cluster. They both listen on the TCP port 443 for HTTP requests from GUI and NBI clients. All clients use the virtual IP (VIP) address of the cluster to access its services. At any time, the VIP address is owned by only one node in the cluster. Hence, the Apache HTTP server on the node that owns the VIP address receives all HTTP requests from GUI and NBI clients and acts as the active load-balancer server, whereas the other server acts as the standby. A round-robin load-balancing algorithm is used to distribute requests to JBoss servers running on all nodes in the cluster. The load-balancer also employs session-stickiness to ensure that all HTTP requests from a user session are sent to the same node in the cluster. To achieve this, the server sets a cookie named JSESSIONID. The value of this cookie identifies the specific node in the cluster that serves requests that belong to this user session. All additional requests contain this cookie and the load-balancer forwards the request to the JBoss server that runs on the node that this cookie identifies.

If the Apache HTTP server on a node goes down, the server is automatically restarted by the watchdog service on that node. If this node owns the VIP address, then the GUI and NBI clients might experience a brief service outage until the Apache HTTP server is restarted. However, this outage lasts only a few seconds (typically, two seconds) and is hardly noticed by the clients. On the other hand, if the Apache HTTP server goes down on the node that does not currently own the VIP address, no side -effects are

noticed by any clients or any other components. The watchdog service restarts the server and the server comes back up in about two seconds.

JBoss Cluster

The JBoss application server runs on all nodes except dedicated database nodes in the Junos Space cluster. The nodes form a single all-active logical cluster and the load-balancer server (described previously) distributes the load across all the nodes. Even if one or more of the JBoss servers in the cluster fails, the application logic still continues to be accessible from the surviving nodes. JBoss servers on all nodes are started with the same configuration and use UDP multicast to detect each other and form a single cluster. JBoss also uses UDP multicast for session replication and caching services across all the nodes.

> **NOTE:** The JBoss server does not run on Fault Monitoring and Performance Monitoring (FMPM) nodes and hosted virtual machines.

When the JBoss server on a node goes down, other nodes in the JBoss cluster detect this change and automatically reconfigure themselves to remove the failed node from the cluster. The time taken by other cluster members to detect a failed JBoss server depends on whether the JBoss server process crashed abnormally or is unresponsive. In the former case, cluster members detect the failure immediately (around two seconds) because their TCP connections to the crashed JBoss server are closed by the operating system. In the latter case, cluster members detect the failure in about 52 seconds. If a JBoss server crashes, the JBoss server is restarted automatically by the watchdog service (jmp-watchdog) running on the node. When the JBoss server comes back up, the JBoss server is automatically discovered by other cluster members and added to the cluster. The JBoss server then synchronizes its cache from the other nodes in the cluster. The typical restart time for the JBoss server is two to five minutes, but it can take more time depending on the number of applications installed, the number of devices being managed, the number of DMI schema versions installed, and so forth.

One JBoss server in the cluster always acts as the primary of the cluster. The main purpose of the primary designation is to host services that are deployed as cluster-wide singletons (HA singletons)—for example, services that must be deployed on only one server in the cluster at any time. Junos Space uses a several services of this type, including the Job Poller service, which provides a single timer for scheduling jobs across the cluster, and the Distributed Resource Manager (DRM) service, which monitors and manages the nodes in the cluster. These services are deployed only on the JBoss server that is designated as the primary.

NOTE: This does not mean that the primary does not host other services. Non-cluster singleton services are also hosted on the primary server. Junos Space is configured such that the first JBoss server that comes up in the cluster becomes the primary. If the primary server goes down, other members in the JBoss cluster detect this and elect a new primary.

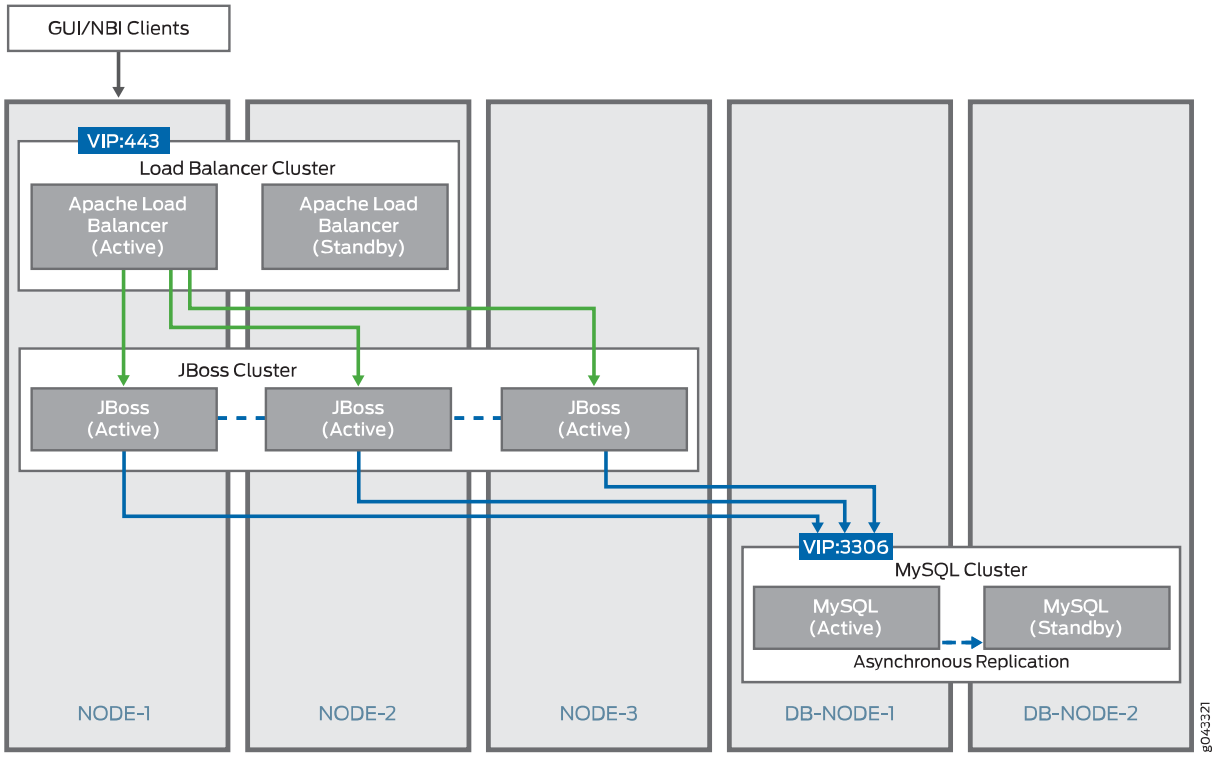
MySQL Cluster

The MySQL server runs on two nodes in the Junos Space cluster at any given time. These nodes form a logical active-standby cluster and both nodes listen on TCP port 3306 for database requests from JBoss servers. By default, JBoss servers are configured to use the Virtual IP (VIP) address of the cluster to access database services. At any time, the VIP address is owned by only one node in the cluster. Thus, the MySQL server on the node that owns the VIP address receives all database requests from the JBoss server, which acts as the active database server while the other server acts as the standby.

If you want to improve the performance of Junos Space Network Management Platform and Junos Space applications, you can add two Junos Space nodes to run as dedicated database nodes. When you add any two Junos Space nodes as the primary and secondary database nodes, the MySQL server is moved to the two dedicated database nodes and is disabled on the first two nodes of the Junos Space cluster. This frees system resources on the Junos Space active VIP node, improving the performance of the node.

JBoss servers use a separate database virtual IP (VIP) address to access database services on dedicated database nodes. You specify the VIP address for the database when you add nodes as dedicated database nodes to the Junos Space cluster. This VIP address is owned by the node designated the primary database node. The MySQL server on the primary database node acts as the active database server, and the server on the secondary database node acts as the standby. Figure 149 shows the logical clusters (Apache Load Balancer cluster, the JBoss cluster, and MySQL cluster) that are formed within a Junos Space cluster when you have dedicated database nodes as part of the Junos Space cluster.

Figure 149: Junos Space Logical Clusters with Dedicated Database Nodes



MySQL servers on each of the nodes are configured with unique server IDs. The primary-/backup relationship is also configured symmetrically on the nodes so that the server on the first node is configured with the second node as the primary; and the server on the second node is configured with the first node as the primary. Thus, both nodes are capable of acting as a backup to the other, and the server running on the node that owns the VIP address acts as the primary at any time, which ensures that the primary-backup relationship switches dynamically as the VIP ownership switches from one node to the other. All transactions committed on the active (primary) server are replicated to the standby (backup) server in near real time, by means of the asynchronous replication solution [2] provided by MySQL, which is based on the binary logging mechanism. The MySQL server operating as the primary (the source of the database changes) writes updates and changes as “events” to the binary log. The information in the binary log is stored in different logging formats according to the database changes that are recorded. The backup server is configured to read the binary log from the primary and to execute all the events in the binary log on the backup's local database.

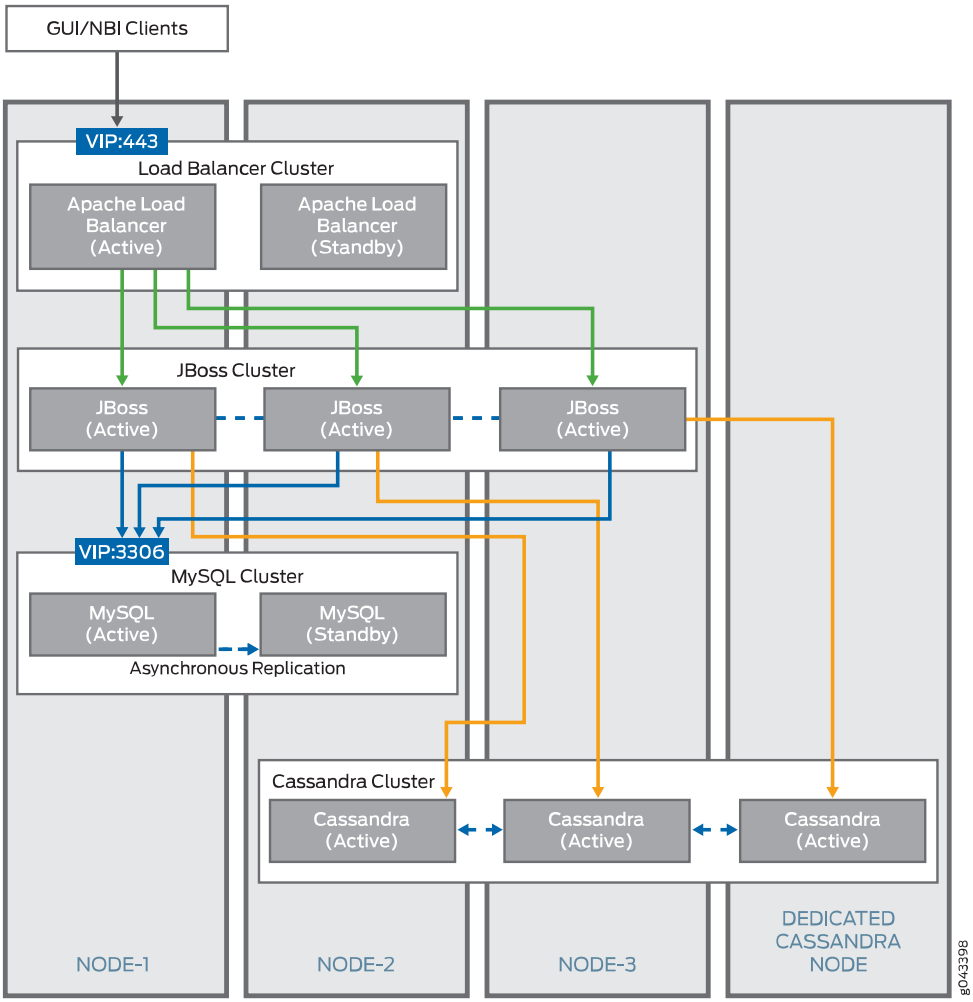
If the MySQL server on a node goes down, the server is restarted automatically by the watchdog service on that node. When restarted, the MySQL server should come up within 20 to 60 seconds. If this node owns the VIP address, JBoss might experience a brief database outage for this 20 to 60 second duration. Any requests that require database access fail during this period. On the other hand, if the MySQL server goes down on the node that does not currently own the VIP address, there are no side- effects noticed by JBoss. The watchdog service restarts the server and the server comes back up in less than one minute.

After the server is back up, it resynchronizes with the primary in the background and the resynchronization time depends on the number of changes that occurred during the outage.

Cassandra Cluster

Starting in Release 15.2R2, Cassandra cluster is an optional logical cluster that you can include within the Junos Space cluster. The Cassandra cluster is formed when there are two or more dedicated Cassandra nodes or two or more JBoss nodes with the Cassandra service running, or a combination of both, within the Junos Space fabric. You can choose to run the Cassandra service on none or all of the nodes in the fabric except dedicated database nodes and FMPM nodes. The Cassandra service running on Junos Space nodes provides a distributed file system to store device images and files from Junos Space applications (such as Juniper Message Bundle [JMB] generated by Service Now and RRD files generated by Network Director). If there are no Cassandra nodes in the fabric, device image files and Junos Space application files are stored in the MySQL database. Figure 150 shows the logical clusters (Apache Load Balancer cluster, JBoss cluster, MySQL cluster, and Cassandra cluster) that are formed within a Junos Space cluster when you have Cassandra nodes as part of the Junos Space cluster.

Figure 150: Junos Space Logical Clusters Including the Cassandra Cluster



The Cassandra service runs on all the Cassandra nodes in an active-active configuration with real-time replication of the Cassandra database. All the files uploaded to the Cassandra database are copied to all the nodes in the Cassandra cluster. JBoss servers send requests to the Cassandra nodes in the Cassandra cluster in a round-robin manner and access the nodes by using the IP address (of the eth0 interface) of the respective Cassandra node.

If any Cassandra node goes down, Junos Space Platform cannot upload files to or delete files from the Cassandra database until the node that is down is deleted from the fabric. If all existing Cassandra nodes are deleted, the files stored in the Cassandra database are lost.

Release History Table

Release	Description
15.2R2	Starting in Release 15.2R2, Cassandra cluster is an optional logical cluster that you can include within the Junos Space cluster.

RELATED DOCUMENTATION

Understanding Virtual IP Availability Within a Junos Space Cluster | 1673

Understanding High Availability Nodes in a Cluster | 1674

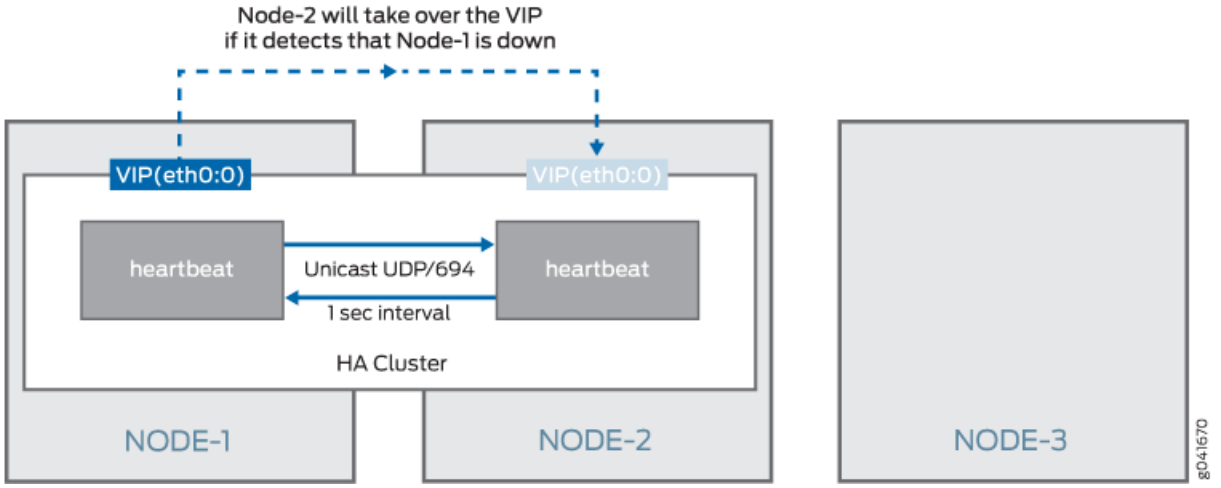
Configuring the Junos Space Cluster for High Availability Overview | 1681

Understanding Virtual IP Availability Within a Junos Space Cluster

Junos Space must ensure that the virtual IP (VIP) address is always available on one of the nodes in the cluster. This is essential for the HA solution because if the VIP address becomes unavailable, the entire cluster becomes unavailable to all user interface clients and NBI clients. To protect against this scenario, Junos Space uses the heartbeat service (version 2.1.3 to version 3) provided by the Linux-HA project to ensure that the VIP address is always available on one of the nodes in the cluster. For information about the Linux-HA project, see the Linux HA User Guide.

Figure 151 shows the heartbeat service that runs on two nodes in the cluster, which together form a Linux HA cluster.

Figure 151: Heartbeat Service on a Linux High Availability Cluster



The heartbeat service is configured symmetrically on both nodes to send a heartbeat message to the other node at a 1-second interval. Unicast messages to UDP port 694 are used to send the heartbeat messages. If a node misses 10 consecutive heartbeat messages from the other node, it will consider the other node as dead and initiate a failover to take ownership of the protected resource. The protected resource in this case is the VIP address of the cluster. When failover occurs, the virtual IP address is obtained using a method known as IP address takeover (for more information, see IP Address Take Over) whereby the newly activated node configures the VIP address on one of its interfaces (eth0:0 is used in Junos Space for this) and sends gratuitous ARP packets for the VIP address. All hosts on the network should receive

these ARP packets and, from this point forward, send subsequent packets for the VIP address to this node. When the node that currently owns the VIP address crashes, an automatic failover of the VIP address to the other node in the cluster occurs in a little more than 10 seconds. When the crashed node comes back up (for example, in the case of a reboot), it joins the HA cluster and acts as the standby node. In other words, an automatic failback of the VIP address does not happen.

> **NOTE:** The 10 seconds that it takes Junos Space to detect a failed node is applicable when the node crashes or becomes nonresponsive. However, in cases where the node is shut down or rebooted, or if the heartbeat service on the node is stopped by the Junos Space administrator, a message is sent to the heartbeat service on the other node and VIP failover occurs almost instantaneously.

In the case of dedicated database nodes, the database VIP address failover happens in a similar manner to ensure database high availability.

RELATED DOCUMENTATION

- Understanding the Logical Clusters Within a Junos Space Cluster | **1666**
- Understanding High Availability Nodes in a Cluster | **1674**
- Configuring the Junos Space Cluster for High Availability Overview | **1681**

Understanding High Availability Nodes in a Cluster

A Junos Space cluster must include at least two nodes to achieve high availability (HA). If the cluster includes more than two nodes, the availability of the cluster does not increase, but the amount of load that the cluster can handle increases with each node added to the cluster. So at any given time, only two nodes in the cluster provide HA to the whole cluster. By default, these two nodes alone (referred to as the HA nodes in the cluster) form the Linux HA cluster, the Apache Load Balancer cluster, and the MySQL cluster. If you have added dedicated database nodes to the cluster, the MySQL cluster is formed by the primary and secondary database nodes.

By default, the first two nodes added to the cluster function as the HA nodes. In the topic "Understanding the Logical Clusters Within a Junos Space Cluster" on page 1666, the example shows that the first two nodes (Node-1 and Node-2) are HA nodes. If you were to delete Node-1 or Node-2 from the **Network Management Platform > Administration > Fabric** workspace, the system checks to see if other nodes in the cluster are available to replace the deleted HA node. The system then displays the list of capable nodes (only Node-3 in the example), which you can select. After you confirm the selected node, the Distributed Resource Manager (DRM) service adds the node to the HA cluster by sending requests to the Node

Management Agent (NMA) running on the newly selected node. The following actions are initiated on the node added to the HA cluster:

- Apache HTTP server with the mod_proxy load balancer is started on the node and the node is configured with all JBoss nodes as members.
- If there are no dedicated database nodes in the cluster, the database from the MySQL server on the other HA node in the cluster is copied and the MySQL server is started on the node. This server is configured as a backup of the other MySQL server in the cluster and it resynchronizes with the primary in the background. The existing MySQL server is also reconfigured to act as a backup of this new server to ensure a symmetric primary/backup configuration on both.

When you add dedicated database nodes to the Junos Space cluster, you add two nodes together as the primary and secondary database nodes to form the MySQL cluster. The database is copied from the active HA node to the two database nodes and is disabled on the HA nodes. If you were to delete one of the database nodes from the cluster, the other database node is designated the primary database node. The system checks whether non-HA nodes in the cluster are available to replace the deleted database node and displays the list of nodes you can select to replace the deleted node.

After you select a node, the Distributed Resource Manager (DRM) service adds the node to the MySQL cluster by sending requests to the Node Management Agent (NMA) running on the newly selected node.

The following actions are initiated on the node added to the MySQL cluster:

- The database from the MySQL server on the primary database node in the cluster is copied and the MySQL server is started on the newly-added secondary database node. This server is configured as a backup of the MySQL server on the primary database node and it resynchronizes with the primary in the background. The existing MySQL server on the primary database node is also reconfigured to act as a backup of this new server on the secondary database node to ensure a symmetric primary/backup configuration on both.
- The JBoss server is stopped on the newly added database node.

In addition to the three default logical clusters, if you have a Cassandra cluster as part of the Junos Space fabric, the files uploaded to Cassandra are copied to all the Cassandra nodes that are part of the Cassandra cluster. Hence, if one Cassandra node fails, the files from the failed node are not lost. However, Junos Space Platform cannot upload files to or delete files in the Cassandra database until the node that failed is deleted.

If the Cassandra service is enabled on an HA node and that node goes down, and if you want to run the Cassandra service on the newly added HA node, you must manually enable and start the Cassandra service on the node. When the last node with the Cassandra service running is deleted, the files stored in the Cassandra database are lost.

RELATED DOCUMENTATION

Understanding the Logical Clusters Within a Junos Space Cluster | 1666

Configuring the Junos Space Cluster for High Availability Overview | 1681

Understanding High Availability Management of DMI Connections

Junos Space maintains a persistent device management interface (DMI) connection with each managed device and supports the following types of DMI connections:

- Space-initiated (default)—A TCP connection from a JBoss server process on a node to the SSH port (22 by default) on the device.
- Device-initiated—A TCP connection from the device to port 7804 on a JBoss server process on a node.

To load balance DMI connections, all connections are distributed across all the nodes in a Junos Space cluster. A device keepalive monitor sends a heartbeat message to devices every 40 seconds. If there is no reply for 15 minutes, the device keepalive monitor marks the connection status of the device as Down.

A device connection monitor scans the connection status of all devices with space-initiated connections. If the monitor detects that the connection status of a device is Down, it attempts to reconnect to the device. If this first attempt fails, a second attempt is made after 30 minutes. Because each reconnect attempt is performed from a node in the cluster that is the least loaded in terms of the number of devices managed, the device might get reconnected from a different node in the cluster after a connection failure.

When devices are discovered using device-initiated connection mode, the device management IP address of all nodes in the Junos Space cluster gets configured in the outbound SSH stanza on the device. The device will keep trying to connect to one of these IP addresses until one succeeds. The device is responsible for detecting any failures on the connection and for reconnecting to another node in the cluster. For more information, see the *Junos XML Management Protocol Guide*.

If a JBoss server process crashes or is stopped, or if the node running the process is shut down, all the DMI connections that it maintains are migrated to another node in the cluster. When this JBoss server comes up, these DMI connections are not automatically migrated back to the JBoss server because it is available for any new devices that are being discovered. At present, there is no way to migrate DMI connections back to this original JBoss server, which can result in poor load balancing of DMI connections if there are not many new devices to be discovered.

RELATED DOCUMENTATION

Understanding High Availability Nodes in a Cluster | 1674

High Availability for Network Monitoring

IN THIS SECTION

- High-Availability Fabric without FMPM Nodes | 1677
- High-Availability Fabric with FMPM Nodes | 1678

The type of Junos Space cluster you create determines how high availability for the network monitoring service functions. A Junos Space fabric without Fault Monitoring and Performance Monitoring (FMPM) nodes uses the two high availability (HA) nodes in the cluster to protect the network monitoring service against node failures. However, when a Junos Space fabric includes one or more FMPM nodes, network monitoring functionality is disabled on the Junos Space nodes and enabled on the FMPM nodes.

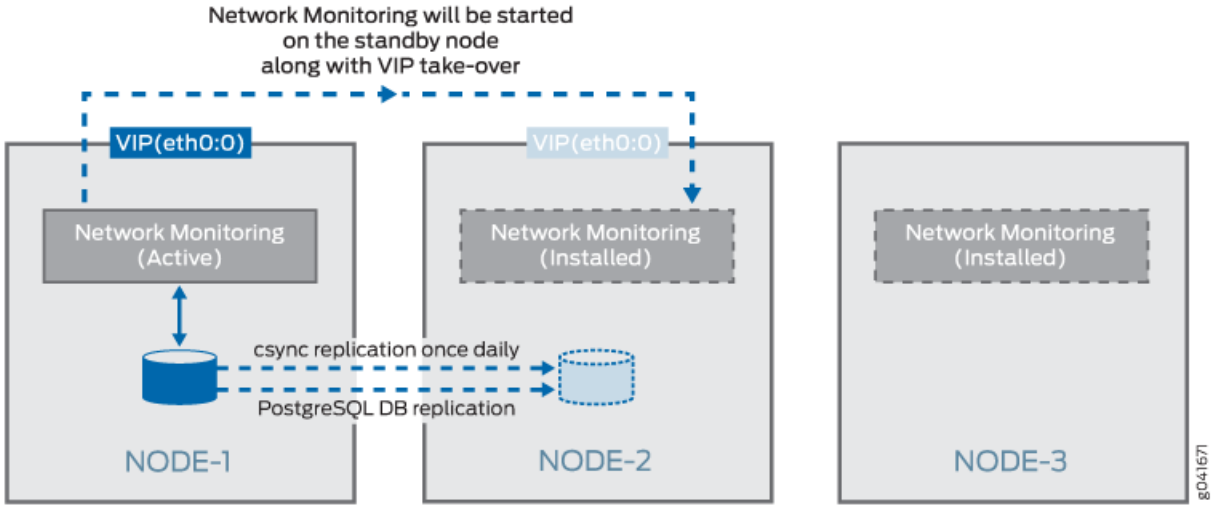
This topic includes the following sections:

High-Availability Fabric without FMPM Nodes

When a Junos Space fabric does not include FMPM nodes, the Junos Space cluster employs a hot-standby solution that uses the two high availability (HA) nodes in the cluster to protect the network monitoring service against node failures.

Figure 152 shows how network monitoring runs on two HA nodes in the cluster to protect the service in the event of node failure.

Figure 152: Linux High Availability Cluster



The network monitoring service is automatically installed on all nodes in the cluster. However, at any time, the network monitoring service runs only on the node that currently owns the virtual IP (VIP) address, and the service is responsible for all fault management and performance management functionality for the entire cluster. Network monitoring uses PostgreSQL 9.1 database for its storage needs. As Figure 152 shows, real-time streaming replication with continuous archiving is set up between the two HA nodes (Node-1 and Node-2 in the cluster), which ensures that the network monitoring database on the standby node is continuously in sync with the network monitoring database on the active node. In addition, a cron job runs on the active node once a day at midnight to synchronize the network monitoring file system to the standby node, which ensures that all back-end configuration files that network monitoring uses are also synchronized between the two HA nodes.

When a VIP failover to the standby node occurs, network monitoring is automatically started on the node. The network monitoring service takes approximately 3 to 5 minutes to complete its initialization before it performs all fault monitoring and performance monitoring functionality for the cluster. Consequently, Junos Space users can expect a network monitoring outage to last approximately 3 to 5 minutes.

The watchdog service on the two HA nodes is responsible for ensuring that the network monitoring service is running on the HA node that owns the virtual IP address and is not running on the other (standby) HA node. As already noted, the watchdog service checks the status of all services on the node every second. If the watchdog service detects that the node owns the VIP address but does not run the network monitoring service, the watchdog service starts the network monitoring service and creates the cron job to synchronize fault management and performance management data to the other node. If the watchdog service detects that the node does not own the VIP address but is running the network monitoring service, the watchdog service shuts down the service and removes the cron job entry for data synchronization.

High-Availability Fabric with FMPM Nodes

If you manage a large or complex network, you might want to dedicate all your performance and network monitoring functionality to a special node called the Fault Monitoring and Performance Monitoring (FMPM) node. When you create a Junos Space fabric with one or more FMPM nodes, network monitoring functionality is disabled on all the Junos Space nodes and enabled on the FMPM nodes. When the first FMPM node is added to the fabric, network monitoring functionality is enabled on this node and the PostgreSQL 9.1 database runs on this node.

When you add a second FMPM node to the fabric, the first FMPM node functions as the primary node, and the second FMPM node functions as the standby node. The network monitoring service is automatically installed on both FMPM nodes in the FMPM team. However, at any time, the network monitoring service runs only on the FMPM node that currently owns the VIP address, and the service is responsible for all fault management (FM) and performance management (PM) functionality for the FMPM team. Network monitoring uses PostgreSQL 9.1 database for its storage needs.

Real-time streaming replication with continuous archiving is set up between the two FMPM nodes in the team, which ensures that the network monitoring database on the standby node is continuously in sync with the network monitoring database on the active node. In addition, a cron job runs on the active FMPM

node once a day at midnight to synchronize the network monitoring file system to the standby FMPM node, which ensures that all back-end configuration files that network monitoring uses are also synchronized between the two FMPM nodes. When a VIP failover to the standby FMPM node occurs, network monitoring is automatically started on the second FMPM node. The network monitoring service takes approximately 3 to 5 minutes to complete its initialization before it performs all FM and PM functionality for the FMPM team. Consequently, Junos Space users can expect a network monitoring outage to last approximately 3 to 5 minutes.

The watchdog service on the two nodes is responsible for ensuring that the network monitoring service is running on the FMPM node which owns the virtual IP address and is not running on the other (standby) FMPM node. As already noted, the watchdog service checks the status of all services on the active FMPM node every second. If the watchdog service detects that the FMPM node owns the VIP address but does not run the network monitoring service, the watchdog service starts the network monitoring service and creates the cron job to synchronize fault management and performance management data to the other node. If the watchdog service detects that the FMPM node does not own the VIP address but is running the network monitoring service, the watchdog service shuts down the service and removes the cron job entry for data synchronization.

RELATED DOCUMENTATION

Understanding How Devices Are Configured to Send SNMP Traps to Junos Space | 1679

Understanding High Availability Nodes in a Cluster | 1674

Configuring the Junos Space Cluster for High Availability Overview | 1681

Understanding How Devices Are Configured to Send SNMP Traps to Junos Space

Devices discovered in Junos Space are automatically configured to send SNMP traps to Junos Space.

The trap destination IP address that is configured on devices depends on whether a separate device management interface (eth3) is used on the node on which network monitoring is currently running. If the node uses the eth3 interface for device management, then the discovered devices are configured with the eth3 IP address. Otherwise, the discovered devices are configured with the virtual IP (VIP) address of the Junos Space cluster. If the VIP is configured as the trap destination, you do not need to reconfigure the trap destination on managed devices after a VIP failover because network monitoring will be started automatically on the node that currently owns the VIP and the node will start receiving the traps. However, if the eth3 IP address is configured as the trap destination, you must reconfigure all devices when a VIP failover occurs. This will be done automatically as part of the startup process of network monitoring on

the second HA node. When network monitoring comes up on the new node, the trap destination on all managed devices will be automatically reconfigured to be the eth3 IP address for this node.

> **NOTE:** Automatic reconfiguration is not possible for devices whose connection with Junos Space is down at the time of the network monitoring failover. If there are any such devices, network monitoring stops receiving traps from these devices after the failover, and you will need to manually change the trap destination on these devices to the eth3 IP address of the node where network monitoring is currently running.

RELATED DOCUMENTATION

High Availability for Network Monitoring | **1677**

Understanding High Availability Nodes in a Cluster | **1674**

CHAPTER 95

Configuring High Availability Overview

IN THIS CHAPTER

- Configuring the Junos Space Cluster for High Availability Overview | 1681

Configuring the Junos Space Cluster for High Availability Overview

IN THIS SECTION

- Requirements | 1681
- Preparation | 1682
- Configuring the First Node in the Cluster | 1684
- Adding a Second Node to the Cluster | 1685
- Adding Additional Nodes to a Cluster | 1685
- Configuring FMPM Nodes | 1686
- Removing Nodes from a Cluster | 1686

This topic provides an overview of the key steps required to configure a Junos Space cluster as a carrier-grade system with all high-availability capabilities enabled.

Requirements

You can choose either Junos Space Appliances (JA2500) or Virtual Appliances for setting up a Junos Space cluster.

For a cluster of Virtual Appliances, the following recommendations apply for the underlying virtualization infrastructure on which the appliances are deployed:

- Use VMware ESX server 4.0 or later or VMware ESXi server 4.0, 5.0, 5.1, 5.5, or 6.0 or a kernel-based virtual machine (KVM) server on qemu-kvm (KVM) Release 0.12.1.2-2/448.el6 or later (which is on CentOS Release 6.5) that can support a virtual machine.
- Deploy the two Junos Space Virtual Appliances (JSVA) on two separate servers.
- Each server must be able to dedicate 4 vCPUs or 2.66 GHz or more, 32 GB RAM, and sufficient hard disk for the Junos Space Virtual Appliance that it hosts.
- The servers should have similar fault tolerance features as the Junos Space appliance: dual redundant power supplies connected to two separate power circuits, RAID array of hard disks for storage, and hot-swappable fans.

> **NOTE:** For more information on the requirements for the virtual appliance, refer to the *Deploying a Junos Space Virtual Appliance on a VMware ESXi Server* and *Deploying a Junos Space Virtual Appliance on a KVM Server* topics in the *Junos Space Virtual Appliance* documentation.

If you choose Junos Space appliances, you need to choose two instances of the corresponding SKUs for the appliance that you are using. In addition, order a second power supply module for each appliance in order to provide the redundant power supply module for each appliance.

Preparation

We recommend you use the following guidelines as you prepare a Junos Space cluster for high availability:

- The Junos Space cluster architecture allows you to dedicate one or two nodes solely for fault monitoring and performance monitoring functions. These are known as Fault Monitoring and Performance Monitoring (FMPM) nodes and are recommended when managing complex networks with a large number of devices and interfaces to be monitored. The advantage of this architecture is that fault and performance monitoring functions are localized within the FMPM nodes and the rest of the Junos Space nodes are freed up for other functions. One of the first decisions that you must make is whether to use FMPM nodes in your Junos Space cluster. If you choose to deploy FMPM nodes, we recommended that you have two of them so that the fault monitoring and performance monitoring services also have high availability. Currently, load balancing is not implemented across multiple FMPM nodes, so there is no need to have more than two FMPM nodes in a cluster.

- The Junos Space cluster architecture allows you to dedicate two Junos Space nodes solely for MySQL database functions. Dedicated database nodes can free up system resources such as CPU time and memory utilization on the Junos Space VIP node, thereby improving the performance of the Junos Space VIP node. If you decide to add dedicated database nodes to the Junos Space cluster, in the first

instance you must add two nodes together as the primary and secondary database nodes, enabling database high availability by default.

- Junos Space Platform enables you to run the Cassandra service on dedicated nodes with only the Cassandra service running or on nodes with the JBoss server running. When the Cassandra service is started on any of the nodes, device images and files from Junos Space applications are moved from the MySQL database to the Cassandra database, thereby improving the performance of the MySQL database. If you want to ensure redundancy for files stored in the Cassandra database, you must ensure that the Cassandra service is running on two or more nodes that together form the Cassandra cluster.

- A Junos Space appliance (hardware or virtual) utilizes two Ethernet interfaces: eth0 and eth3. The eth0 interface is used for all inter-node communication within the cluster and also for communication between GUI and NBI clients and the cluster. The eth3 interface can be configured as the device management interface, in which case, all communication between the cluster and the managed devices occur over this interface. If the eth3 interface is not configured, all device communication also takes place over the eth0 interface. So, you must first decide whether or not to use eth3 as the device management interface. If you choose to use eth3, you should use eth3 for all appliances in the same cluster.

- You also must decide on the following networking parameters to be configured on the Junos Space appliances:

  - IP address and subnet mask for the interface “eth0”, the default gateway address, and the address of one or more name servers in the network.
  - IP address and subnet mask for the interface “eth3” if you choose to use a separate device management interface.
  - The virtual IP address to use for the cluster, which should be an address in the same subnet as the IP address assigned to the “eth0” interface.

    If you decide to add dedicated database nodes, you must choose a separate virtual IP (VIP) address in the same subnet as the VIP address of the Junos Space cluster. This database VIP address must be in the same subnet as the IP address assigned to the eth0 Ethernet interface and must be different from the VIP address of the Junos Space cluster and the FMPM nodes.

    If you decide to use an FMPM cluster, you must choose a separate virtual IP address for the FMPM nodes. Please note that the FMPM virtual IP address need not be in the same subnet as the virtual IP address of the Junos Space nodes.
  - NTP server settings from which to synchronize the appliance’s time.

- The IP address that you assign to each Junos Space node in the cluster and the virtual IP address for the cluster must be in the same subnet. This is required for the IP address takeover mechanism to function correctly.

  It is possible to configure the FMPM nodes in a separate subnet.

> **NOTE:** Strictly speaking, you can choose to deploy the non-HA nodes in a different subnet. However, doing so will cause a problem if one of the HA nodes goes down and you want to promote one of the other nodes as an HA node. So, we recommend that you configure eth0 on all nodes in the same subnet.

- Because JBoss servers on all the nodes communicate using UDP multicast to form and manage the JBoss cluster, you must ensure that UDP multicast is enabled in the network where you deploy the cluster nodes. You must also disable IGMP snooping on the switches interconnecting the cluster, or configure them explicitly to allow UDP multicast between the nodes.

  > **NOTE:** FMPM nodes and dedicated database nodes do not participate in the JBoss cluster. Therefore, there is no need to enable UDP multicast between these nodes and the Junos Space nodes in the cluster.

Configuring the First Node in the Cluster

After you power on the appliance and connect to its console, Junos Space displays a menu-driven command-line interface (CLI) that you use to specify the initial configuration of the appliance. To complete this initial configuration, you specify the following parameters:

- IP address and subnet mask for the interface “eth0”
- IP address of the default gateway
- IP address of the name server
- IP address and subnet mask for the interface “eth3”, if you choose to configure a cluster as described in the topic “Understanding the Logical Clusters Within a Junos Space Cluster” on page 1666.
- Whether this appliance being added to an existing cluster. Choose “n” to indicate that this is the first node in the cluster.
- The virtual IP address that the cluster will use.
- NTP server settings from which to synchronize the appliance’s time.
- Maintenance mode user ID and password.

> **NOTE:** Make note of the user ID and password that you specify for maintenance mode, as you will need this ID and password to perform Network Management Platform software upgrades and database restoration.

For detailed step-by-step instructions on configuring the appliance for initial deployment, refer to the Junos Space appliance documentation. After you have completed the initial configuration, all Junos Space services are started on the appliance and you can log in to the Network Management Platform User Interface from the virtual IP address assigned to it. At this stage, you have a single node cluster with no HA, which you can see by navigating to the **Network Management Platform > Administration> Fabric** workspace.

Adding a Second Node to the Cluster

In order to add a second node to the cluster, you must first configure the second appliance using its console. The process is identical to that of the first appliance except that you need to choose “y” when it you are prompted to specify whether this appliance will be added to an existing cluster. Make sure that the IP address you assign to this node is in the same subnet as the first node. You must also ensure its uniformity in using a separate device management interface (eth3). If you chose to use eth3 for the first node, choose the same for all additional nodes in the cluster.

After you configure the second appliance, you can log in to the Network Management Platform user interface of the first node at its virtual IP address to add the node to the cluster from the **Network Management Platform > Administration > Fabric > Add Fabric Node** workspace. To add the node to the cluster, specify the IP address assigned to the eth0 interface of the new node, assign a name for the new node, and (optionally) schedule the date and time to add the node. The Distributed Resource Manager (DRM) service running on the first node contacts Node Management Agent (NMA) on the new node to make necessary configuration changes and add it to the cluster. The DRM service also ensures that required services are started on this node. After the new node joins the cluster, you can monitor its status from the **Network Management Platform > Administration > Fabric** workspace.

For more information about adding nodes to an existing cluster from the Junos Space Platform UI, see “Fabric Management Overview” on page 1157 (in the *Junos Space Network Management Platform Workspaces User Guide*).

Adding Additional Nodes to a Cluster

The process for adding additional nodes is identical to the process for adding the second node. However, these additional nodes do not participate in any of the HA clusters in the fabric, unless explicitly promoted to that role if another HA node is removed, or if they are added as dedicated database nodes to form the MySQL cluster.

For more information about adding nodes to an existing cluster from the Junos Space Platform UI, see "Fabric Management Overview" on page 1157 (in the *Junos Space Network Management Platform Workspaces User Guide*).

Configuring FMPM Nodes

You can configure up to 2 FMPM nodes in a cluster. To configure FMPM nodes:

- For Junos Space appliances, refer to the following topics in the *Hardware Documentation* section of the *Junos Space Network Management Platform* documentation:
  - *Configuring a Junos Space Appliance as a Standalone or Primary FMPM Node*
  - *Configuring a Junos Space Appliance as a Backup or Secondary FMPM Node for High Availability*
- For Junos Space Virtual Appliances, refer to the following topics in the *Junos Space Virtual Appliance* documentation:
  - *Configuring a Junos Space Virtual Appliance as a Standalone or Primary FMPM Node*
  - *Configuring a Junos Space Virtual Appliance as a Backup or Secondary FMPM Node for High Availability*

Removing Nodes from a Cluster

If a node has failed and needs to be replaced, you can easily remove the node from the cluster. Navigate to the **Network Management Platform > Administration > Fabric** workspace, select the node you want to remove, and choose the **Delete Node** action. If the node being deleted is an HA node, the system will check if other nodes in the cluster can be elected as the replacement for the HA node being deleted. The system then shows the list of capable nodes (only Node-3 in this example) and allows you to choose from the available nodes. The process is described in "Understanding High Availability Nodes in a Cluster" on page 1674.

If the node being deleted is a database node, the system checks whether other nodes in the cluster can replace the database node being deleted. If there are nodes present that are capable of replacing the deleted node, the system displays the list of capable nodes and allows you to choose from the available nodes.

For more information about deleting nodes from the cluster, see "Deleting a Node from the Junos Space Fabric" on page 1259 (in the *Junos Space Network Management Platform Workspaces User Guide*).

RELATED DOCUMENTATION

Understanding High-Availability Failover Scenarios | 1687

CHAPTER 96

High Availability Failover Scenarios

IN THIS CHAPTER

- Understanding High-Availability Failover Scenarios | **1687**

Understanding High-Availability Failover Scenarios

IN THIS SECTION

- Active VIP Node Crashes | **1688**
- Standby VIP Node Crashes | **1688**
- eth0 on the Active VIP Node Goes Down | **1689**
- eth0 on the Standby VIP Node Goes Down | **1690**
- A Non-VIP Node Crashes | **1690**
- eth0 on a Non-VIP Node Goes Down | **1690**
- eth3 on a Non-VIP Node Goes Down | **1691**
- eth3 on the Active VIP Node Goes Down | **1691**
- JBoss Server on a Node Goes Down | **1692**
- MySQL Server on the Active VIP Node Goes Down | **1693**
- MySQL Server on the Standby VIP Node Goes Down | **1693**
- Primary Database Node Crashes | **1694**
- Secondary Database Node Crashes | **1694**
- MySQL Server on the Primary Database Node Goes Down | **1694**
- MySQL Server on the Secondary Database Node Goes Down | **1695**
- Apache HTTP Server on the Active VIP Node Goes Down | **1695**
- Apache HTTP Server on the Standby VIP Node Goes Down | **1696**
- Dedicated Cassandra Node Crashes | **1696**
- Cassandra Service on a JBoss Node Goes Down | **1696**

The following sections describe possible high-availability failure scenarios: how a failure is detected, what recovery action to take, and if applicable, the impact on the system caused by the failure.

Active VIP Node Crashes

Detection

The heartbeat service running on a standby VIP node detects a crash within 10 seconds of not receiving any heartbeat messages from its peer. The JBoss clustering mechanism enables JBoss servers on other nodes to detect that the JBoss server on the failed node is unresponsive, in about 52 seconds.

Recovery

The standby node immediately takes over the VIP address.

Device connections served by the failed node are migrated to the remaining nodes in the cluster. This process starts in about one minute after the JBoss cluster members detect that the JBoss server on the failed node is down. The time it takes for the process to complete depends on the number of device connections to be migrated, the load on the remaining nodes, and so on. Typically, the process is completed within a few minutes.

After the VIP address is taken over by the standby node, a network monitoring service is started on the standby node. It takes around three to five minutes for the network monitoring service to complete its initialization. It might take more time depending on the size of the FM and PM data that is being maintained.

Impact

The VIP address becomes unavailable for about 10 seconds until it is taken over by the standby node. The GUI or API client access during this period encounters transient errors. In addition, any SNMP traps sent by the devices to the VIP address during this interval are lost.

Device connectivity is down for a few minutes for devices whose connections were being served by the JBoss server on the failed node.

Any jobs that were in progress on the failed node are marked as failed and the reason is indicated.

Users experience an outage of network monitoring functionality for about three to five minutes while the network monitoring service is being initialized on the standby node.

Standby VIP Node Crashes

Detection

The JBoss clustering mechanism enables JBoss servers on the other nodes to detect that the JBoss server on the failed node is unresponsive in about 52 seconds.

Recovery

Device connections served by the failed node are migrated to the remaining nodes in the cluster. This process starts in about one minute after the JBoss cluster members detect that the JBoss server on the failed node is down. The process completion time depends on the number of device connections to be migrated, the load on the remaining nodes, and so on. Typically, this process is completed within a few minutes.

Impact

Device connectivity is down for a few minutes for devices whose connections were being served by the JBoss server on the failed node.

Any jobs that were in progress on the failed node are marked as failed and the reason is indicated.

eth0 on the Active VIP Node Goes Down

Detection

The heartbeat service running on the standby VIP node detects the crash within 10 seconds of not receiving any heartbeat messages from its peer. The JBoss clustering mechanism enables JBoss servers on the other nodes to detect that the JBoss server on the failed node is unresponsive, in about 52 seconds.

Recovery

The standby node immediately takes over the VIP address.

Device connections served by the failed node are migrated to the remaining nodes in the cluster. This process starts in about one minute after the JBoss cluster members detect that the JBoss server on the failed node is down. The time it takes for the process to complete depend on the number of device connections to be migrated, the load on the remaining nodes, and so on. Typically, the process is completed within a few minutes.

After the VIP address is taken over by the standby node, a network monitoring service is started on the standby node. It takes around three to five minutes for the network monitoring service to complete its initialization. It might take more time depending on the size of FM and PM data that is being maintained.

Impact

The VIP address becomes unavailable for about 10 seconds until it is taken over by the standby node. The GUI or API client access during this period encounters transient errors. In addition, any SNMP traps sent by the devices to the VIP address during this interval are lost.

Device connectivity is down for a few minutes for the devices whose connections were being served by the JBoss server on the failed node.

Any jobs that were in progress on the failed node are marked as failed and the reason is indicated.

Users experience an outage of network monitoring functionality for about three to five minutes while the network monitoring service is being initialized on the standby node.

eth0 on the Standby VIP Node Goes Down

Detection

The JBoss clustering mechanism enables JBoss servers on the other nodes to detect that the JBoss server on the failed node is unresponsive in about 52 seconds.

Recovery

Device connections served by the failed node are migrated to the remaining nodes in the cluster. This process starts in about one minute after the JBoss cluster members detect that the JBoss server on the failed node is down. The process completion time depends on the number of device connections to be migrated, the load on the remaining nodes, and so on. Typically, this process is completed within a few minutes.

Impact

Device connectivity is down for a few minutes for the devices whose connections were being served by the JBoss server on the failed node.

Any jobs that were in progress on the failed node are marked as failed and the reason is indicated.

A Non-VIP Node Crashes

Detection

The JBoss clustering mechanism enables JBoss servers on the other nodes to detect that the JBoss server on the failed node is unresponsive in about 52 seconds.

Recovery

Device connections served by the failed node are migrated to the remaining nodes in the cluster. This process starts in about one minute after the JBoss cluster members detect that the JBoss server on the failed node is down. The time it takes for the process to complete depends on the number of device connections to be migrated, the load on the remaining nodes, and so on. Typically, this process is completed in a few minutes.

Impact

Device connectivity is down for a few minutes for devices whose connections were served by the JBoss server on the failed node. Any jobs that were in progress on the failed node are marked as failed and the reason is indicated.

eth0 on a Non-VIP Node Goes Down

Detection

The JBoss clustering mechanism enables JBoss servers on the other nodes to detect that the JBoss server on the failed node is unresponsive in about 52 seconds.

Recovery

Device connections served by the failed node are migrated to the remaining nodes in the cluster. This process starts in about 1one minute after the JBoss cluster members detect that the JBoss server on the failed node is down. The process completion time depends on the number of device connections to be migrated, the load on the remaining nodes, and so on. Typically, this process is completed in, a few minutes.

Impact

Device connectivity is down for a few minutes for the devices whose connections were being served by the JBoss server on the failed node.

Any jobs that were in progress on the failed node are marked as failed and the reason is indicated.

eth3 on a Non-VIP Node Goes Down

Detection

The device keepalive monitor detects that all device connections served by this node are down in 15 minutes and marks the connection status of these devices as Down.

Recovery

For connections initiated by Junos Space , Junos Space attempts to reconnect with these devices. Each attempt is made from the cluster node that is determined to be the least loaded in terms of the number of devices it manages. If other nodes in the cluster are significantly less loaded than this node, according to this load-balancing check, reconnection attempts are made from those nodes and they succeed. In this case, connectivity for these devices comes back up in a few minutes. If this node happens to be the least loaded, then all reconnection attempts are made from this node and these attempts continue to fail as long as eth3 remains down.

In the case of device-initiated connections, the device detects a connection failure in about 15 minutes, and then reconnects with another node in the cluster in the next few seconds.

Impact

Device connectivity is down for devices whose connections were being served by this node. Connectivity might be down for 15 minutes (best case) or until eth3 is brought back up (worst case). In addition, the outage time might vary from device to device depending on which node is chosen to attempt a reconnection for that device. In the case of device-initiated connections, the outage lasts for a little more than 15 minutes.

eth3 on the Active VIP Node Goes Down

Detection

The device keepalive monitor detects that all device connections served by this node are down in 15 minutes and marks the connection status of these devices as Down.

Recovery

For Jconnections initiated by Junos Space, Junos Space attempts to reconnect with these devices. Each attempt is made from the cluster node that is determined to be the least loaded in terms of the number of devices it manages. If other nodes in the cluster are significantly less loaded than this node, according to this load-balancing check, reconnection attempts are made from those nodes and they succeed. In this case, connectivity for these devices comes back up in a few minutes. If this node happens to be the least loaded, then all reconnection attempts are made from this node and these attempts continue to fail as long as eth3 remains down.

In the case of device-initiated connections, the device detects a connection failure in about 15 minutes and then reconnects with another node in the cluster in the next few seconds.

Impact

Device connectivity is down for the devices whose connections were being served by this node. Connectivity might be down for 15 minutes (best case) or until eth3 is brought back up (worst case). In addition, the outage time might vary from device to device depending on which node is chosen to attempt a reconnection for that device. In the case of device-initiated connections, the outage lasts for a little more than 15 minutes.

The network monitoring service is also affected because it runs only on the VIP node. The service does not receive any SNMP traps from any managed device because all devices are configured with the eth3 IP address of the VIP node as the trap destination. In addition, all performance and fault monitoring of all managed devices fail until eth3 is brought back up.

JBoss Server on a Node Goes Down

Detection

When the JBoss server on a node goes down, other nodes in the JBoss cluster detect the failure in about two seconds) because their TCP connections to the failed JBoss server are closed by the operating system.

Recovery

Device connections served by the failed JBoss server are migrated to the other nodes in the cluster. This process starts in about one minute after the JBoss cluster members detect that the JBoss server on the failed node is down. The time it takes for the process to complete depends on the number of device connections to be migrated, the load on the remaining nodes, and so on. Typically, the process is completed within a few minutes.

The watchdog service (jmp-watchdog) running on the node detects that the JBoss server is down and restarts it automatically. When the JBoss server comes back up, it is automatically discovered by other cluster members and added to the cluster. It then synchronize its cache from the other nodes in the cluster. The typical restart time for JBoss is two to five minutes. However, it can take more time depending on

the number of applications installed, the number of devices being managed, the number of DMI schema versions installed, and so on.

Impact

Device connectivity is down for a few minutes for devices whose connections were being served by the JBoss server that went down.

Any jobs that were in progress on the crashed JBoss server are marked as failed and the reason is indicated.

MySQL Server on the Active VIP Node Goes Down

Detection

If the MySQL server on a node goes down, the watchdog service detects the down MySQL server on that active node in about one to two seconds.

Recovery

The watchdog service immediately restarts the MySQL server on the node. When restarted, the MySQL server comes up in around 20 to 60 seconds.

Impact

The MySQL server on the VIP node is the active database servicing all requests from all JBoss servers in the cluster. This effectively means that a brief database outage could be experienced by JBoss on all nodes for this duration (20 to 60 seconds). Any requests that require database access fail during this period. This results in failures encountered by GUI or API clients on their requests, which internally require database access during this period. This also results in failures of jobs that require database access during this period.

MySQL Server on the Standby VIP Node Goes Down

Detection

If the MySQL server on a node goes down, the watchdog service detects the down MySQL server on that standby node in about one to two seconds.

Recovery

The watchdog service immediately restarts the MySQL server on the node. When restarted, it takes around 20 to 60 seconds for the MySQL server to come up. After it is back up, this server resynchronizes with the primary server in the background and the resynchronization time depends on the number of changes that happened during the outage.

Impact

Since the MySQL server on the standby VIP node is not accessed by JBoss, its downtime does not cause any adverse impact that is noticed by the rest of the system or users of the system.

Primary Database Node Crashes

Detection

The heartbeat service running on the secondary database node detects the crash within 10 seconds of not receiving any heartbeat messages from the primary database node.

Recovery

The database VIP address is transferred to the secondary database node within 10 to 20 seconds. The JBoss servers on other nodes can access the database after the database VIP address is taken over by the secondary database node.

Impact

The database VIP address becomes unavailable for about 10 to 20 seconds until it is taken over by the secondary database node.The MySQL server on the primary database node is the active database servicing all requests from all JBoss servers in the cluster. This effectively means that a brief database outage could be experienced by JBoss on all nodes for this duration (20 to 60 seconds). Any requests that require database access fail during this period. This results in failures encountered by GUI and API clients on their requests that internally require database access during this period. This also results in failures of jobs that require database access during this period.

Secondary Database Node Crashes

Detection

The heartbeat service running on the primary database node detects the crash within 10 seconds of not receiving any heartbeat messages from the secondary database node.

Recovery

The node can be deleted and a new node can be added to the Junos Space cluster as a secondary database node to maintain database high availability.

Impact

Because the MySQL server on the secondary database node is not accessed by JBoss, its downtime does not cause any adverse impact that is noticed by the rest of the system or users of the system.

MySQL Server on the Primary Database Node Goes Down

Detection

If the MySQL server on a node goes down, the watchdog service detects the down MySQL server on that active node in about one to two seconds.

Recovery

The watchdog service immediately restarts the MySQL server on the node. When restarted, the MySQL server comes up in around 20 to 60 seconds.

Impact

The MySQL server on the primary database node is the active database servicing all requests from all JBoss servers in the cluster. This effectively means that a brief database outage could be experienced by JBoss on all nodes for this duration (20 to 60 seconds). Any requests that require database access fail during this period. This results in failures encountered by GUI and API clients on their requests that internally require database access during this period. This also results in failures of jobs that require database access during this period.

MySQL Server on the Secondary Database Node Goes Down

Detection

If the MySQL server on a node goes down, the watchdog service detects the down MySQL server on that standby node in about one to two seconds.

Recovery

The watchdog service immediately restarts the MySQL server on the node. When restarted, it takes around 20 to 60 seconds for the MySQL server to come up. After it is back up, this server resynchronizes with the primary database node in the background. The resynchronization time depends on the number of changes that happened during the outage.

Impact

Because the MySQL server on the secondary database node is not accessed by JBoss, its downtime does not cause any adverse impact that is noticed by the rest of the system or users of the system.

Apache HTTP Server on the Active VIP Node Goes Down

Detection

If the Apache HTTP server on a node goes down, the watchdog service detects the down HTTP server on that node in about one to two seconds.

Recovery

The watchdog service immediately restarts the Apache HTTP server on the node and it becomes ready for service in one second.

Impact

A brief service outage could be experienced by GUI and NBI clients until the Apache HTTP server is restarted. However, this outage is only for a few seconds (typically, two seconds) and is hardly noticed by the clients.

Apache HTTP Server on the Standby VIP Node Goes Down

Detection

If the Apache HTTP server on a node goes down, the watchdog service detects the down HTTP server on that node in about one to two seconds.

Recovery

The watchdog service immediately restarts the Apache HTTP Server on the node and it becomes ready for service in one second.

Impact

No impact.

Dedicated Cassandra Node Crashes

Detection

If the Cassandra node goes down, the watchdog service detects that the Cassandra service is down on that node in about one to two seconds.

Recovery

The Cassandra node that is down must be deleted from the fabric.

Impact

Files cannot be uploaded to or deleted from the Cassandra database until the node that is down is deleted from the fabric.

Cassandra Service on a JBoss Node Goes Down

Detection

If the Cassandra service on a JBoss node goes down, the watchdog service detects that the Cassandra service is down on that node in about one to two seconds.

Recovery

The Cassandra service on the node must be disabled.

Impact

Files cannot be uploaded to or deleted from the Cassandra database until the Cassandra service is disabled on the node.

RELATED DOCUMENTATION

Configuring the Junos Space Cluster for High Availability Overview | **1681**

Disaster Recovery Overview | **1699**

PART 17

Disaster Recovery

Disaster Recovery Solution | **1699**

Configuring the Disaster Recovery Process | **1731**

Managing the Disaster Recovery Solution | **1747**

Upgrading Junos Space Network Management Platform with Disaster Recovery Enabled | **1789**

CHAPTER 97

Disaster Recovery Solution

IN THIS CHAPTER

- Disaster Recovery Overview | 1699
- Understanding the Normal Operation of Active and Standby Sites | 1723
- Understanding Disaster Recovery Failure Scenarios | 1724
- Understanding How the Standby Site Becomes Operational When the Active Site Goes Down | 1730

Disaster Recovery Overview

IN THIS SECTION

- Disaster Recovery Solution | 1700
- Prerequisites to Configure Disaster Recovery | 1702
- Connectivity Requirements to Configure Disaster Recovery | 1703
- Disaster Recovery Watchdog | 1703
- Failure Detection by Using the Device Arbitration Algorithm | 1706
- Failure Detection by Using the Custom Failure-Detection Scripts | 1707
- Steps to Configure Disaster Recovery | 1718
- Disaster Recovery Commands | 1719

A Junos Space cluster allows you to maintain high availability and scalability in your network management solution. However, because all nodes in a cluster need to be within the same subnet, they are typically deployed in the same data center or within the same campus. But you can easily recover a cluster from a disaster at a location by mirroring the original Junos Space installation on a cluster to another cluster at a geographically different location. So if the main Junos Space site fails due to a disaster such as an earthquake, the other site can take over. Hence, the physical installation of the disaster recovery setup is typically a set of two geographically separate clusters: the active or main site (that is, the local site) and the standby or backup site (that is, the remote site).

When the basic connectivity requirements and prerequisites are met (refer to “Prerequisites to Configure Disaster Recovery” on page 1702 and “Connectivity Requirements to Configure Disaster Recovery” on page 1703), data from the cluster at the active site is replicated to the cluster at the standby site in near realtime.

The data in the MySQL and PgSQL databases is replicated asynchronously from the active site to the standby site over an SSL connection. MySQL and PgSQL data between the disaster recovery sites is encrypted using self-signed SSL certificates that are generated when disaster recovery is initialized. CA root certificate, CRLs, user certificates, scripts, device images, archived audit logs, and information about scheduled jobs are replicated to the standby site during the real-time data replication to the standby site. The configuration and round-robin database (RRD) files are synchronized periodically by using Secure Copy Protocol (SCP) from the active site to the standby site.

The disaster recovery watchdog, an in-built Junos Space mechanism, monitors the integrity of database replication across sites. All other services (such as JBoss, OpenNMS, Apache, and so on) do not run on the standby site until the active site fails over to the standby site. A failover to the standby site is automatically initiated when the active site is down. A device arbitration algorithm is used to determine which site should be the active site to prevent a split-brain scenario where both sites try to be active. For information about the device arbitration algorithm, see “Failure Detection by Using the Device Arbitration Algorithm” on page 1706.

The following sections describe the connectivity requirements for the disaster recovery process, failure-detection mechanisms, and the disaster recovery commands:

Disaster Recovery Solution

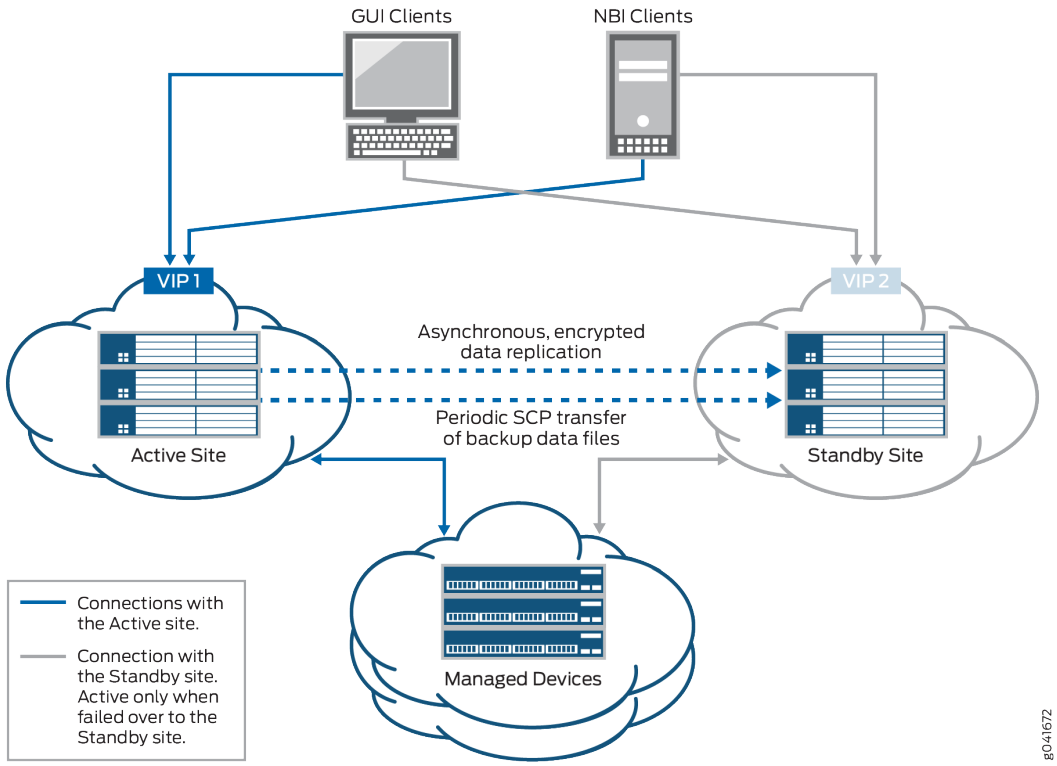
After you configure and initiate the disaster recovery process between an active site and a standby site, asynchronous replication of MySQL and PgSQL database between the sites is initiated. Configuration and RRD files are backed up to the standby site through SCP at defined time intervals.

The disaster recovery process does not perform real-time replication of the Cassandra database to the standby site or monitor the Cassandra service running on the Junos Space nodes.

During the normal operation of the disaster recovery solution, the GUI and API users and the managed devices are connected to the active site for all network management services. The connectivity between the standby site and managed devices is disabled as long as the active site is functional. When the active site becomes unavailable due to a disaster, the standby site becomes operational. At this time, all services on the standby site are started and the connectivity between the standby site and managed devices is established.

Figure 153 displays the disaster recovery solution.

Figure 153: Disaster Recovery Solution



The disaster recovery watchdog process is initiated at the VIP node of both the active and standby sites to monitor the health of the replication process and detect when the remote site goes down. The disaster recovery watchdog at the local site checks whether there are connectivity issues between both sites (by pinging the nodes at the remote site) and whether the sites are connected to arbiter devices (if you use the device arbitration algorithm).

The disaster recovery watchdog at a site performs the following tasks to confirm connectivity with the remote site and arbiter devices:

- Ping the VIP address of the remote site at a regular configurable interval. The default value for the interval is 30 seconds.

  For each ping, expect a reply within a configurable timeout interval. The default value for the timeout interval is 5 seconds.

- If the local site fails to receive a reply within the timeout interval, the disaster recovery watchdog retries the ping for a configurable number of times. By default, the number of retries is 4.

- If all the retries fail, the disaster recovery watchdog at the local site concludes that the VIP address of the remote site is not reachable.

  However, the disaster recovery watchdog does not conclude that the remote site is down because the remote site may be switching over the VIP address to a standby node due to a local switchover.

- To consider the possibility of a VIP address switchover, the disaster recovery watchdog pings the IP addresses of the other load-balancer nodes at the remote site. If the ping to any of the nodes receives a reply, the disaster recovery watchdog concludes that the remote site is still up.

  If the ping to the nodes fails, the disaster recovery watchdog does not conclude that the remote site is down. Instead, the disaster recovery watchdog considers the possibility of connectivity issues between the sites. Both sites will try to become active.

- To prevent both sites from trying to become active, the disaster recovery watchdog initiates the device arbitration algorithm and determines whether a failover is required.

  A failover is initiated only if the percentage of arbiter devices managed by the active site falls below the failover threshold. Then the active site becomes the standby site and the standby site becomes the active site.

  If the percentage of arbiter devices is above the failover threshold, the standby site remains standby and the active site remains active. The percentage of arbiter devices managed by the active site is configurable and its default value is 50%.

The failover is initiated if the following conditions are met:

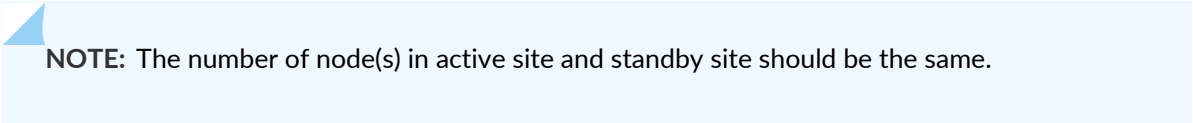
- The standby site cannot reach the VIP address of the active site or the node IP addresses of other load-balancer nodes at the active site.
- The percentage of the arbiter devices managed by the active site is below the failover threshold.

For more information about the device arbitration algorithm, see "Failure Detection by Using the Device Arbitration Algorithm" on page 1706.

Prerequisites to Configure Disaster Recovery

You need to ensure that your Junos Space installation meets the following prerequisites before you configure disaster recovery:

- The Junos Space cluster at the primary or active site (which can be a single node or multiple nodes) and the cluster at the remote or standby site (which can be a single node or multiple nodes) must be set up in exactly the same way, with all the same applications, device adapters, same IP family configurations, and so on.
- Both clusters should be configured with SMTP server information from the Junos Space user interface. For more information, see "Managing SMTP Servers" on page 1477. This configuration enables the clusters at both the active site and the standby site to notify the administrator by e-mail if the replications fail.



Connectivity Requirements to Configure Disaster Recovery

You need to ensure that the disaster recovery solution meets the following connectivity requirements before you configure disaster recovery:

- Layer 3 connectivity between the Junos Space clusters at the active and standby sites. This means:
  - Every node in a cluster can successfully ping the VIP address of the other cluster
  - Every node in a cluster can use SCP to transfer files between the active and standby sites
  - Database replication across the two clusters is possible through TCP ports 3306 (MySQL database replication) and 5432 (PostgreSQL database replication)
  - The bandwidth and latency of the connection between the two clusters are such that real-time database replication is successful. Although the exact bandwidth required depends on the amount of data transferred, we recommend a minimum of a 100-Mbps bandwidth connection with a latency of fewer than 150 milliseconds.
- Independent Layer 3 connectivity between each cluster and managed devices
- Independent Layer 3 connectivity between each cluster and GUI or NBI clients

To set up the disaster recovery process, see "Configuring the Disaster Recovery Process Between an Active and a Standby Site" on page 1731.

Disaster Recovery Watchdog

IN THIS SECTION

- heartbeat | **1704**
- mysqlMonitor | **1704**
- pgsqlMonitor | **1704**
- fileMonitor | **1705**
- arbiterMonitor | **1705**
- configMonitor | **1705**
- serviceMonitor | **1705**
- notification | **1705**

The disaster recovery watchdog, also known as a DR watchdog, is an in-built Junos Space mechanism to monitor the integrity of data replication (MySQL database, PgSQL database, configuration files, and RRD files) across sites. The disaster recovery watchdog also monitors the overall health of the disaster recovery

setup, initiates a failover from the active to the standby site when the active site fails, and enables the standby site to resume network management services with minimal service disruption. An instance of the disaster recovery watchdog is initiated at the VIP node on both sites when you start the disaster recovery process.

The disaster recovery watchdog provides the following services:

heartbeat

The heartbeat service between the active and standby sites uses ping to check the connectivity between the sites. Both sites send heartbeat messages to each other. The heartbeat service performs the following tasks:

- Detect a failure at the remote site by pinging the remote site at regular intervals.
- When the remote site fails to reply, rule out the possibility of a temporary issue due to a local failover at the remote site.
- Enable or disable automatic failover depending on the disaster recovery configuration settings.
- Avoid split-brain scenarios by running the device arbitration algorithm (default) or the logic configured in the custom script.
- Verify the disaster recovery configuration after a site is rebooted.

mysqlMonitor

The mysqlMonitor service performs the following tasks:

- Monitor the health of MySQL database replication within the site and between the active and standby sites.
- Fix MySQL database replication errors.
- Notify the administrator through e-mail if any of the MySQL database replication errors cannot be fixed automatically.

pgsqlMonitor

The pgsqlMonitor service performs the following tasks:

- Monitor the health of PgSQL database replication within the site and between the active and standby sites.
- Fix PgSQL database replication errors.
- Notify the administrator through e-mail if any of the PgSQL database replication errors cannot be fixed automatically.

fileMonitor

The fileMonitor service performs the following tasks:

- Monitor the health of the configuration files and RRD files replicated within the sites and between the active and standby sites.
- Fix errors found during the replication of configuration files and RRD files.
- Notify the administrator through e-mail if any of the replication errors cannot be fixed automatically. You can also view the replication errors in the output of the cron job.

arbiterMonitor

The arbiterMonitor service periodically checks whether the local site can ping all the arbiter devices. If the percentage of arbiter devices that are reachable falls below a configured warning threshold (70%, by default), an e-mail notification is sent to the administrator.

configMonitor

The configMonitor service performs the following tasks:

- Monitor the disaster recovery configuration files at all nodes at both sites.
- Transfer the configuration files across nodes within a site if the files are not in sync.

serviceMonitor

The serviceMonitor service performs the following tasks:

- Monitor the status of selected services (such as jboss, jboss-dc, httpd, and dr-watchdog) within a specific site.
- Start or stop the selected services if they display an incorrect status.

notification

The notification service notifies the administrator about error conditions, warnings, or disaster recovery state changes detected by the disaster recovery watchdog through e-mail. Notification e-mails are sent if:

- Automatic failover is disabled due to connectivity issues between a site and arbiter devices.
- The percentage of arbiter devices that are reachable is lower than the warning threshold.
- A site becomes standby or active.
- The standby site cannot back up files from the active site through SCP.
- A site cannot establish an SSH connection to the remote site.
- The local site cannot fetch the hostname of the MySQL primary node.
- A site cannot fix MySQL and PgSQL database replication errors.

The notification service does not send e-mails to report the same errors within a configurable period of time (by default, 3600 seconds).

Failure Detection by Using the Device Arbitration Algorithm

A device arbitration algorithm is used to detect failure at a site. A list of highly reachable devices running Junos OS and managed by Junos Space Platform are selected as arbiter devices. We recommend that you select arbiter devices based on the following criteria:

- You must be able to reach the arbiter devices through Junos Space–initiated SSH connections from both sites. Do not select devices that use device-initiated connections to Junos Space Platform.
- You must be able to ping arbiter devices from both disaster recovery sites.
- You must choose arbiter devices that stay connected to Junos Space Platform or are less frequently rebooted or shut down because this may impact the device arbitration algorithm results. If you foresee that certain arbiter devices will be offline during some part of their lives, avoid choosing those devices.
- You must choose arbiter devices from different geographical locations to ensure that a problem in the management network at a location does not make all arbiter devices unreachable from your sites.
- You cannot select NAT and ww Junos OS devices as arbiter devices.

The device arbitration algorithm at the active site uses ping to connect to arbiter devices from the active site. The device arbitration algorithm at the standby site logs in to the arbiter devices through SSH connections by using the login credentials from the Junos Space Platform database. Following are the workflows of the device arbitration algorithm at the active and standby sites.

At the active site:

1. Ping all selected arbiter devices.
2. Compute the percentage of arbiter devices that can be pinged.
3. Check whether the percentage of arbiter devices that can be pinged is above or the same as the configured value of the failover threshold.
    - If the percentage of arbiter devices connected is above or the same as the configured value of the failover threshold (failureDetection.threshold.failover parameter in the watchdog section of the disaster recovery API), failover is not initiated because the active site is managing a majority of the arbiter devices.
    - If the percentage of arbiter devices is below the configured value of the failover threshold, failover is initiated (if automatic failover is enabled) and the active site becomes standby. If automatic failover is disabled, the active site remains active.

At the standby site:

1. Log in to arbiter devices through SSH connections.
2. Execute a command on each arbiter device to retrieve the list of SSH connections to any node (managed by the node) at the active site.
3. Calculate the percentage of arbiter devices managed by the active site.
4. Calculate the percentage of arbiter devices that cannot be reached through SSH connections.
   - If the percentage of arbiter devices managed by the active site is above or the same as the configured value of the failover threshold, failover is not required because the active site is still managing a majority of the arbiter devices.
   - If the percentage of arbiter devices managed by the active site is below the configured value of the failover threshold, the disaster recovery watchdog concludes that a failover may be required.
5. However, because the devices that cannot be reached from the standby site may be connected and managed by the active site, the standby site assumes that all arbiter devices that cannot be reached are being managed by the active site and calculates the new percentage of devices managed by the active site.
   - If the percentage of devices managed by the active site is below the threshold percentage to adjust managed devices (failureDetection.threshold.adjustManaged parameter in the watchdog section of the disaster recovery API, the default value is 50%), the standby site remains standby. By default, the threshold percentage to adjust managed devices must be below the failover threshold.
   - If the new percentage calculated by adding the devices managed by the active site and arbiter devices that cannot be reached is below the failover threshold, the disaster recovery watchdog concludes that a failover must be initiated.

     If automatic failover is enabled, the standby site initiates the process of becoming active. If automatic failover is disabled, no failover happens.

If you disabled automatic failover or the feature was disabled due to connectivity issues, you must execute **jmp-dr manualFailover** at the standby site to resume network management services from the standby site.

Failure Detection by Using the Custom Failure-Detection Scripts

In addition to using the device arbitration algorithm, you can create custom failure-detection scripts (sh, bash, Perl, or Python) to decide when or whether to fail over to the standby site. Custom failure scripts invoke the **jmp-dr api v1 config ––include** command and fetch the disaster recovery configuration and the status of the disaster recovery watchdog services. The disaster recovery configuration and the status of the disaster recovery watchdog services at a site are organized as various sections. Table 207 lists these sections.

Use the **-- include <section-name>** option to view the details of a section or use the details of the section in the custom failure-detection script.

Table 207: API Sections

Section	Description	Details Included in the Section	Sample Output
role	Disaster recovery role of the current site	Roles can be active, standby, or standalone.	–
failover	Type of failover that happened last	Value can be active_to_standby, standby_to_active, or empty if failover has not happened yet.	–

core	Core disaster recovery configuration that includes the remote site node details	peerVip–VIP of the load-balancer at the remote site
		
		adminPass–Encrypted administrator passwords of the remote site. Multiple entries are separated by commas.
		
		scpTimeout–Timeout value used to detect SCP transfer failures between sites
		
		peerLoadBalancerNodes–Node IP addresses of the load-balancer nodes at the remote site. Multiple entries are separated by commas.
		
		peerBusinessLogicNodes–Node IP addresses of the JBoss nodes at the remote site. Multiple entries are separated by commas.
		
		peerDeviceMgtIps–Device management IP addresses of the remote site. Multiple entries are separated by commas.
			<pre>{
			"core": {
			"peerVip": "10.155.90.210",
			
			"adminPass": "ABCDE12345",
			"scpTimeout": 120,
			"peerLoadBalancerNodes":
			"10.155.90.211",
			"peerBusinessLogicNodes":
			"10.155.90.211",
			"peerDeviceMgtIps":
			"10.155.90.211"}
			}</pre>

Table 207: API Sections *(continued)*

Section	Description	Details Included in the Section	Sample Output
mysql	Disaster recovery configuration related to the MySQL database at the remote site	hasDedicatedDb–Whether the remote site includes dedicated database nodes peerVip–VIP of the MySQL nodes at the remote site (either normal node or dedicated database node) peerNodes–Node IP addresses of the MySQL nodes at the remote site (either normal node or dedicated DB node). Multiple entries are separated by commas.	`{ "mysql": { "hasDedicatedDb": false, "peerVip": "10.155.90.210", "peerNodes": "10.155.90.211" } }`
pgsql	Disaster recovery configuration related to the PgSQL database at the remote site	hasFmpm–Whether the remote site includes specialized FMPM nodes peerFmpmVip–VIP of the PostgreSQL nodes at the remote site (either normal node or FM/PM specialized node) peerNodes–Node IP addresses of the PostgreSQL nodes at the remote site (either normal node or FM/PM specialized node). Multiple entries are separated by commas.	`{ "psql": { "hasFmpm": false, "peerFmpmVip": "10.155.90.210", "peerNodes": "10.155.90.211" } }`
file	Configuration and RRD files–related disaster recovery configuration at the remote site	backup.maxCount–Maximum number of backup files to retain backup.hoursOfDay–Times of the day to back up files backup.daysOfWeek–Days of the week to back up files restore.hoursOfDay–Times of the day to poll files from the active site restore.daysOfWeek–Days of the week to poll files from the active site	`{ "file": { "backup": { "maxCount": 3, "hoursOfDay": "*", "daysOfWeek": "*" }, "restore": { "hoursOfDay": "*", "daysOfWeek": "*" } } }`

Table 207: API Sections *(continued)*

Section	Description	Details Included in the Section	Sample Output

watchdog	Disaster recovery configuration related to the disaster recovery watchdog at the current site	heartbeat.retries–Number of times to retry the heartbeat message
		
		heartbeat.timeout–Timeout of each heartbeat message in seconds
		
		heartbeat.interval–Heartbeat message interval between sites in seconds
		
		notification.email–Contact e-mail address to report service issues
		
		notification.interval–Dampening interval between receiving e-mails about affected services
		
		failureDetection.isCustom–Whether the remote site uses custom failure detection
		
		failureDetection.script–Path of the failure-detection script
		
		failureDetection.threshold.failover–Threshold percentage to trigger a failover
		
		failureDetection.threshold.adjustManaged–Threshold percentage to adjust the percentage of managed devices
		
		failureDetection.threshold.warning–Threshold percentage to send a warning to ensure that a disaster recovery site can reach more arbiter devices to improve the accuracy of the device arbitration algorithm
		
		failureDetection.waitDuration–Grace period to allow the original active site to become active again when both sites become standby
		
		failureDetection.arbiters–List of arbiter devices
			{ "watchdog": {
			"heartbeat": {
			"retries": 4,
			"timeout": 5,
			"interval": 30 },
			"notification": {
			"email":
			"abc@example.com",
			"interval": 3600 },
			"failureDetection": {
			"isCustom": false,
			"script":
			"/var/cache/jnp-geo/watchdog/bin/arbitration",
			
			"threshold": {
			"failover": 0.5,
			"adjustManaged": 0.5,
			"warning": 0.7 },
			"waitDuration": "8h",
			"arbiters": [{
			"username": "user1",
			"password": "xxx",
			"host":
			"10.155.69.114",
			"port": 22,
			"privateKey": ""
			}]
			}
			}
			}

Table 207: API Sections *(continued)*

Section	Description	Details Included in the Section	Sample Output
deviceManagement	Device management IP addresses at the remote site	peerNodes–Device management IP addresses of the remote site. Multiple entries are separated by commas. nodes–Device management IP addresses at the current site. Multiple entries are separated by commas. ip–Device management IP address and interface on this node (node on which the **jmp-dr api v1 config --list** command is executed)	`{ "deviceManagement": { "peerNodes": "10.155.90.211", "nodes": "10.155.90.222", ”ip”: “10.155.90.228,eth0” } }`

Table 207: API Sections *(continued)*

Section	Description	Details Included in the Section	Sample Output

states	Runtime information of the disaster recovery watchdog services at the current site. If the disaster recovery watchdog has never run on this site, this section is not available. If the disaster recovery watchdog has stopped, the information in this section is out-of-date.	–	<pre>{ "states": {
			  "arbiterMonitor": {
			  "progress": "idle",
			  "msg": {
			  "service": "arbiterMonitor",
			  "description": "",
			  "state": true,
			  "force": false,
			  "progress": "unknown",
			  "payload": {
			  "code": 0
			  },
			  "time": "2015-07-18T22:18:55+00:00"
			  },
			"service": {}
			  },</pre>

			<pre> "configMonitor": {
			  "progress": "idle",
			  "msg": {
			  "service": "configMonitor",
			  "description": "",
			  "state": true,
			  "force": false,
			  "progress": "unknown",
			  "payload": {
			  "code": 0
			  },
			  "time": "2015-07-18T22:19:15+00:00"
			  },"service": {}
			  },</pre>

Table 207: API Sections *(continued)*

Section	Description	Details Included in the Section	Sample Output

			<pre>"fileMonitor": {
			"progress": "idle",
			"msg": {
			"service":
			"fileMonitor",
			"description": "",
			"state": true,
			"force": false,
			"progress":
			"unknown",
			"payload": {
			"code": 0
			},
			"time":
			"2015-07-18T22:18:59+00:00"
			},
			"service": {}
			},</pre>

Table 207: API Sections *(continued)*

Section	Description	Details Included in the Section	Sample Output

			<pre>"heartbeat": {
			"progress": "unknown",
			"msg": {
			"service":
			"heartbeat",
			"description": "",
			"state": true,
			"force": false,
			"progress":
			"unknown",
			"payload": {
			"localFailover":
			false
			},
			"time":
			"2015-07-18T22:17:49+00:00"
			},
			"service": {
			"booting": false,
			"bootEndTime": null,
			"waitTime": null,
			"automaticFailover":
			false,
			
			"automaticFailoverEndTime":
			"2015-07-18T07:41:41+00:00"
			}
			},</pre>

Table 207: API Sections *(continued)*

Section	Description	Details Included in the Section	Sample Output

			<pre>"mysqlMonitor": {
			"progress": "idle",
			"msg": {
			"service":
			"mysqlMonitor",
			"description": "",
			"state": true,
			"force": false,
			"progress":
			"unknown",
			"payload": {
			"code": 0
			},
			"time":
			"2015-07-18T22:19:09+00:00"
			},
			"service": {}
			},</pre>

			<pre>"pgsqlMonitor": {
			"progress": "unknown",
			"msg": {
			"service":
			"pgsqlMonitor",
			"description":
			"Master node pgsql in active
			or standby site maybe
			CRASHED. Pgsql replication is
			in bad status. Please
			manually check Postgresql-9.4
			status.",
			"state": false,
			"force": false,
			"progress":
			"unknown",
			"payload": {
			"code": 1098
			},
			"time":
			"2015-07-18T22:18:27+00:00"
			},"service": {}
			},</pre>

Table 207: API Sections *(continued)*

Section	Description	Details Included in the Section	Sample Output

			<pre>"serviceMonitor": {
			"progress": "running",
			"msg": {
			"service":
			"serviceMonitor",
			"description": "",
			"state": true,
			"force": false,
			"progress":
			"unknown",
			"payload": {
			"code": 0
			},
			"time":
			"2015-07-18T22:19:30+00:00"
			},
			
			"service": {}
			}
			}
			}</pre>

The output from the custom script informs the disaster recovery watchdog whether a failover to the standby site is required. The disaster recovery watchdog interprets the output from the script in the JSON format. The following is an example:

```
{
  "state": "active",
  "action": "nothing",
  "description": "",
  "payload": {
    "waitTime": "",
    "details": {
      "percentages": {
        "connected": 1,
        "arbiters": {
          "10.155.69.114": "reachable"
```

```
        }
      }
    }
  }
}
```

Table 208 describes the details of the script output.

Table 208: Details of the Custom Script Output

Property	Description	Data Type	Values or Format	Other Details
state	Current disaster recovery role of this site	String	active standby	Required An empty string is not allowed.
action	Action that the disaster recovery watchdog must perform	String	beActive–Change role to active. beStandby–Change role to standby. nothing–Do not change role. wait–Wait in the current role for the time specified in the payload.waitTime property.	Required An empty string is not allowed.
description	Description of the action field and the message that is sent in the e-mail notification	String	–	Required An empty string is allowed.
payload.waitTime	End time of the grace period when both sites become standby	String (Date)	YYYY-MM-DD, UTC time in HH:MM+00:00 format	Required An empty string is allowed. This property is used when you specify the value of action as wait.

Table 208: Details of the Custom Script Output *(continued)*

Property	Description	Data Type	Values or Format	Other Details
payload.details	User- customized information that can be used to debug the script	–	JSON object	Optional An empty string is not allowed.

Steps to Configure Disaster Recovery

To configure disaster recovery between an active site and a standby site:

1. Stop the disaster recovery process configured during earlier releases before upgrading to Junos Space Network Management Platform Release 15.2R1. For more information on the upgrade process, see the Upgrade Instructions section in the Junos Space Network Management Platform Release Notes 15.2R1.

   For more information about stopping the disaster recovery process configured during earlier releases, see "Stopping the Disaster Recovery Process on Junos Space Network Management Platform Release 14.1R3 and Earlier" on page 1743.

   You do not require to perform this step for a clean installation of Junos Space Network Management Platform Release 15.2R1.

2. Set up SMTP servers at both sites from the Junos Space user interface to receive notifications. For more information, see "Managing SMTP Servers" on page 1477 in the *Junos Space Network Management Platform Workspaces User Guide*.

3. Copy the file with the list of arbiter devices (if you are using the device arbitration algorithm) or the custom failure-detection script to the appropriate location at the active site. Ensure that all arbiter devices are discovered at the active site. For more information, see "Device Discovery Profiles Overview" on page 220 in the *Junos Space Network Management Platform Workspaces User Guide*.

4. Configure the disaster recovery configuration file at the active site. The disaster recovery configuration includes SCP settings to synchronize configuration and RRD files, heartbeat settings, notifications settings, and the failure-detection mechanism.

5. Configure the disaster recovery configuration file at the standby site. The disaster recovery configuration includes SCP settings to synchronize configuration and RRD files, heartbeat settings, and notification settings.

6. Start the disaster recovery process from the active site.

For more information, see "Configuring the Disaster Recovery Process Between an Active and a Standby Site" on page 1731.

Disaster Recovery Commands

You use the disaster recovery commands listed in Table 209 to configure and manage disaster recovery sites. You must execute these commands at the VIP node of the site. You can use the **--help** option with these commands to view more information.

Table 209: Disaster Recovery Commands

Command	Description	Options
jmp-dr init	Initialize the disaster recovery configuration files at both sites. You need to enter values for the parameters prompted by the command. Create MySQL and PgSQL users and passwords required to replicate data and monitor the replication across disaster recovery sites. The following users are created: • User with a default username repUser and password repPass for MySQL database replication. • User with a default username repAdmin and password repAdminPass to monitor the MySQL database replication health and failover. • User with default username replication and password replication for PgSQL replication. • User with default username postgres and password postgres to monitor PgSQL replication health and failover.	**-a**–Initialize the disaster recovery configuration file only at the active site. **-s**–Initialize the disaster recovery configuration file only at the standby site.

Table 209: Disaster Recovery Commands *(continued)*

Command	Description	Options
jmp-dr start	Start the disaster recovery process at both sites. You must execute this command at the VIP node of the active site. The active site establishes an SSH connection to the standby site and executes the **jmp-dr start** command at the standby site. When you execute this command, MySQL database and PgSQL database replication and configuration and RRD files backup to the standby site are initiated. You execute this command: • To initially start the disaster recovery process • To restart the disaster recovery process after you stopped the process to upgrade your Junos Space setup.	**-a**–Start the disaster recovery process only at the active site. **-s**–Start the disaster recovery process only at the standby site.
jmp-dr toolkit config update	When the command is executed without options, the command: • Displays the modified cluster configuration at a site and updates this at the local site. • Accepts and updates the modified cluster configuration at the remote site. You must execute the command in the following order: 1. Accept and update the cluster configuration changes at both sites. 2. Update load-balancer changes, and modify and update SCP timeout settings at both sites. 3. Modify and update other disaster recovery configuration parameters. You must execute this command at the VIP node of the local site to modify the configuration and the VIP node of the remote site to accept the modified configuration.	Use these options to modify the disaster recovery configuration at a site and update the change at the peer site: **-user-core**–Modify the VIP address, password, and SCP timeout settings. **-user-file-backup**–Modify configuration and RRD files backup settings. **-user-file-restore**–Modify configuration and RRD files replication to standby site settings. **-user-watchdog-heartbeat**–Modify disaster recovery watchdog heartbeat settings. **-user-watchdog-notification**–Modify e-mail notification settings. **-user-watchdog-failureDetection**–Modify failure-detection settings.

Table 209: Disaster Recovery Commands *(continued)*

Command	Description	Options
jmp-dr health	Check the status of the disaster recovery process. The command checks whether MySQL and PgSQL databases are replicated and configuration and RRD files are backed up, and verifies the status of the disaster recovery watchdog and reports errors.	–
jmp-dr stop	Stop the disaster recovery process between sites. When you execute this command, MySQL and PgSQL database replication and configuration and RRD files backup between sites are stopped. The disaster recovery data files are not deleted. The status of services such as JBoss, OpenNMS, Apache remains unchanged.	–
jmp-dr reset	Stop the disaster recovery process and delete the disaster recovery data files from a site. The site initiates services as a standalone cluster. You must execute this command at the VIP node of both sites to stop the disaster recovery process completely and delete the disaster recovery data files from both sites.	–
jmp-dr manualFailover	Manually fail over to the standby site. When you execute this command, the standby site becomes the new active site and the active site becomes the new standby site.	**-a**–Manually change the role of the site to active. **-s**–Manually change the role of the site to standby.

Table 209: Disaster Recovery Commands *(continued)*

Command	Description	Options
jmp-dr toolkit watchdog status [options]	Enable automatic failover to the standby site or disable automatic failover to the standby site for a specified duration. **NOTE:** You can execute this command only if the disaster recovery watchdog is active at the site.	**–enable-automatic-failover**–Enable automatic failover to the standby site.
		–disable-automatic-failover *duration*–Disable automatic failover to the standby site for a specified time duration. Enter the time duration in hours or minutes. For example, 1h or 30m. If you do not enter “h” or “m” along with the value—for example, 2—the default duration is calculated in hours. If you enter zero, automatic failover is disabled permanently.
jmp-dr api v1 config	View the disaster recovery configuration and runtime information in the JSON format.	**--list**–View specific sections of the disaster recovery configuration and status of the disaster recovery watchdog services. Table 207 lists the section names.
		--include<*sections*>–Include specific sections of the disaster recovery configuration and status of the disaster recovery watchdog services in the custom failure-detection script. Separate multiple section names with commas. When you include this command in a custom failure-detection script, the command fetches the disaster recovery configuration and status of the disaster recovery watchdog services and executes the logic in the script.

RELATED DOCUMENTATION

- Understanding High Availability Nodes in a Cluster | **1674**
- Configuring the Junos Space Cluster for High Availability Overview | **1681**
- Configuring the Disaster Recovery Process Between an Active and a Standby Site | **1731**
- Modifying Applications and Nodes on a Disaster Recovery Setup | **1765**

Understanding the Normal Operation of Active and Standby Sites

During the normal operation of the active and standby sites, you use the virtual IP (VIP) address of the active site to access its GUI and API for all network management services. On the active site, a cron job is run based on the disaster recovery configuration. MySQL and PgSQL databases at the active site are asynchronously replicated at the standby site. This ensures that if the active site fails due to a disaster, the databases at the standby site contain the most recent data from the active site. Performance monitoring data in the RRD files and certain configuration files are periodically backed up at the active site and transferred to the standby site by using scripts that are configured to run as cron jobs.

To view the cron job to back up files at the active site, execute the **crontab -l** command at the active site. The following is a sample output:

```
[user1@host]# crontab -l
*/5 * * * *  /usr/bin/purgingPolicy.sh >> /var/log/purgingPolicy.log 2>&1
0 */3 * * *  perl /var/www/cgi-bin/mysqlAnalyze.pl >> /var/log/mysqlAnalyze.log 2>&1
0 0 * * *       /opt/opennms/contrib/failover/scripts/sync.sh >>
/opt/opennms/logs/failover.log 2>&1
0 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23 * * 0,1,2,3,4,5,6
 /var/cache/jmp-geo/backup/script/backupReal.sh >>
/var/cache/jmp-geo/backup/backup.log 2>&1
```

The output shows the time you scheduled to run backups at the active site.

The backup is archived into a **tgz** file in the **/var/cache/jmp-geo/backup/data** directory. Only the most recent three backups (default value) or as configured in the disaster recovery configuration are retained in this directory. The older backups are purged. To view a log of all backups by using the **backupReal.sh** script, see the **backup.log** file located at **/var/cache/jmp-geo/backup**.

To view the cron job to fetch files from the active site, execute the **crontab -l** command at the standby site. The following is a sample output:

```
[user1@host]# crontab -l
*/5 * * * *  /usr/bin/purgingPolicy.sh >> /var/log/purgingPolicy.log 2>&1
0 */3 * * *  perl /var/www/cgi-bin/mysqlAnalyze.pl >> /var/log/mysqlAnalyze.log 2>&1
0 0 * * *       /opt/opennms/contrib/failover/scripts/sync.sh >>
/opt/opennms/logs/failover.log 2>&1
0 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23 * * 0,1,2,3,4,5,6
 /var/cache/jmp-geo/restore/script/poll.sh >> /var/cache/jmp-geo/restore/restore.log
 2>&1
```

The output shows the time you scheduled to restore the backups from the active site.

The **poll.sh** script transfers the most recent backup file from the active site using SCP. The backup files are stored in the **/var/cache/jmp-geo/restore/data** directory. The script ensures that only the most recent three backups (default value) or as configured in the disaster recovery configuration are retained in this directory and older files are purged. To view a log of all backups from the active site by using the **poll.sh** script, see the **restore.log** file located at **/var/cache/jmp-geo/restore**.

You cannot discover or manage any devices at the standby site during the normal operation of a disaster recovery setup.

RELATED DOCUMENTATION

- Disaster Recovery Overview | **1699**
- Understanding How the Standby Site Becomes Operational When the Active Site Goes Down | **1730**
- Configuring the Disaster Recovery Process Between an Active and a Standby Site | **1731**

Understanding Disaster Recovery Failure Scenarios

IN THIS SECTION

- Active Site (site1) Goes Down Due to a Disaster or Is Powered Down | **1725**
- No Connectivity Between the Active and Standby Sites and Both Sites Lose Connectivity with Arbiter Devices | **1725**
- No Connectivity Between the Active and Standby Sites | **1726**
- No Connectivity Between the Active and Standby Sites and the Active Site (site1) Loses Connectivity with Arbiter Devices | **1727**
- No Connectivity Between the Active and Standby Sites and the Standby Site (site2) Loses Connectivity With Arbiter Devices | **1727**
- Standby Site (site2) Goes Down Due to Disaster or Is Powered Down | **1728**
- No Connectivity Between the Active Site (site1) and Arbiter Devices | **1729**
- No Connectivity Between the Standby Site (site2) and Arbiter Devices | **1729**

The following sections explain failure scenarios such as the active and standby sites (with automatic failover enabled) going down due to a disaster, losing connectivity between sites, and losing connectivity with arbiter devices. The device arbitration algorithm is used for failure detection.

For the scenarios, assume that the active site is site1 and standby site is site2.

Active Site (site1) Goes Down Due to a Disaster or Is Powered Down

Detection

The disaster recovery watchdog at site2 does not receive replies to successive ping retries to site1. The disaster recovery watchdog at site2 initiates the device arbitration algorithm and finds that arbiter devices (all or most) are not managed by site1.

An e-mail is sent to the administrator with this information.

Impact

MySQL and PgSQL database replication to site2 is stopped. If you configured any file transfers through SCP during downtime, site2 may lose that version of configuration and RRD files.

MySQL and PgSQL databases at site2 now contain the latest data that was replicated in real time from site1 before it went down. This includes configuration, inventory, alarm-related data of all managed devices, and data maintained by Junos Space Platform and Junos Space applications. The latest version of configuration and RRD files available at site2 are from the most recent file transfer through SCP.

Junos Space users and NBI clients need to wait until site2 becomes active and use the VIP address of site2 to access all network management services.

Recovery

The disaster recovery watchdog at site2 initiates the process to become active. The complete process may take around 15 to 20 minutes. This can vary depending on the number of devices that are managed on your Junos Space setup.

When the failover is complete, site2 establishes connections with all devices and resynchronizes configuration and inventory data if required. site2 starts receiving alarms and performance management data from managed devices.

> **NOTE:** When you rebuild or power on site1, if the disaster recovery configuration is deleted, you must reconfigure disaster recovery between the sites.

No Connectivity Between the Active and Standby Sites and Both Sites Lose Connectivity with Arbiter Devices

Detection

The disaster recovery watchdog at both sites do not receive replies to successive ping retries. The disaster recovery watchdog at both sites initiates the device arbitration algorithm.

An e-mail is sent to the administrator regarding the failure of MySQL and PgSQL replication and file transfer through SCP between sites.

Impact

MySQL and PgSQL database replication to site2 is stopped. If you configured any file transfers through SCP during downtime, site2 may lose that version of configuration and RRD files.

Because both sites cannot connect to arbiter devices (all or most), both sites cannot determine the status of the other site. site1 starts to become standby and site2 remains standby to avoid a split-brain situation.

Even if connectivity between the two sites is restored, both sites remain standby because the sites cannot connect to arbiter devices.

The network management services are stopped at both sites until one of the sites becomes active.

If connectivity to arbiter devices is not restored within the grace period (by default, eight hours), automatic failover functionality is disabled at both sites. An e-mail is sent every hour to the administrator with this information.

Recovery

If connectivity to arbiter devices is restored within the grace period (by default, eight hours), site1 becomes active again. site2 remains standby.

If both sites are standby, enable disaster recovery by executing the **jmp-dr manualFailover –a** command at the VIP node of site1. To enable automatic failover at the sites, execute the **jmp-dr toolkit watchdog status --enable-automatic-failover** command at the VIP node of site1 and site2.

Fix connectivity issues between site1 and site2 to resume MySQL and PgSQL replication and file transfer through SCP.

No Connectivity Between the Active and Standby Sites

Detection

The disaster recovery watchdog at both sites do not receive replies to successive ping retries. The disaster recovery watchdog at both sites initiates the device arbitration algorithm and finds that arbiter devices (all or most) are managed by site1.

An e-mail is sent to the administrator regarding the failure of MySQL and PgSQL database replication and file transfer through SCP between sites.

Impact

MySQL and PgSQL database replication to site2 is stopped. If you configured any file transfers through SCP during downtime, site2 may lose that version of configuration and RRD files.

Recovery

site1 remains active and site2 remains standby. Fix connectivity issues between site1 and site2 to resume MySQL and PgSQL database replication and file transfer through SCP.

No Connectivity Between the Active and Standby Sites and the Active Site (site1) Loses Connectivity with Arbiter Devices

Detection

The disaster recovery watchdog at both sites do not receive replies to successive ping retries. The disaster recovery watchdog at both sites initiates the device arbitration algorithm.

An e-mail is sent to the administrator regarding the failure of MySQL and PgSQL database replication and file transfer through SCP between sites.

Impact

MySQL and PgSQL database replication to site2 is stopped. If you configured any file transfers through SCP during downtime, site2 may lose that version of configuration and RRD files.

Because site1 cannot connect to arbiter devices, site1 starts to become standby. Because site2 finds that arbiter devices (all or most) are not managed by site1, a failover is initiated. As part of becoming standby, all network management services are stopped at site1.

site2 now contains the latest MySQL and PgSQL data that was replicated in real time from site1. The latest version of configuration and RRD files available at site2 are from the most recent file transfer through SCP.

Junos Space users and NBI clients need to wait until site2 becomes active and use the VIP address of site2 to access all network management services.

Recovery

The disaster recovery watchdog at site2 initiates the process to become active. The complete process may take around 15 to 20 minutes. This can vary depending on the number of devices that are managed on your Junos Space setup.

When the failover is complete, site2 establishes connections with all devices and resynchronizes configuration and inventory data if required. site2 starts receiving alarms and performance management data from managed devices.

Fix connectivity issues between site1 and site2 to resume MySQL and PgSQL database replication and file transfer through SCP.

No Connectivity Between the Active and Standby Sites and the Standby Site (site2) Loses Connectivity With Arbiter Devices

Detection

The disaster recovery watchdog at both sites do not receive replies to successive ping retries. The disaster recovery watchdog at site1 initiates the device arbitration algorithm and finds that arbiter devices (all or most) are managed by site1. The disaster recovery watchdog at site2 initiates the device arbitration algorithm.

An e-mail is sent to the administrator regarding the failure of MySQL and PgSQL replication and file transfer through SCP between sites.

Impact

MySQL and PgSQL database replication to site2 is stopped. If you configured any file transfers through SCP during downtime, site2 may lose that version of configuration and RRD files.

Because site2 cannot connect to arbiter devices (all or most), site2 remains standby.

site2 retries to connect to arbiter devices, but does not become active again even if it can connect to enough arbiter devices within eight hours. During these eight hours, site2 requests disaster recovery runtime information of the remote site to ensure that the remote site is active and not in the process of a failover. If site2 cannot connect to enough arbiter devices within eight hours, site2 disables automatic failover permanently until you manually enable automatic failover. An e-mail is sent every hour to the administrator with this information.

Recovery

Fix connectivity issues between site1 and site2 to resume MySQL and PgSQL database replication and file transfer through SCP.

To enable automatic failover at the standby site, execute the **jmp-dr toolkit watchdog status --enable-automatic-failover** command at the VIP node of site2.

Standby Site (site2) Goes Down Due to Disaster or Is Powered Down

Detection

The disaster recovery watchdog at site1 does not receive replies to successive ping retries to site2. The disaster recovery watchdog at site1 initiates the device arbitration algorithm and finds that arbiter devices (all or most) are managed by site1.

An e-mail is sent to the administrator regarding the failure of MySQL and PgSQL replication and file transfer through SCP between sites.

Impact

MySQL and PgSQL database replication to site2 is stopped. If you configured any file transfers through SCP during downtime, site2 may lose that version of configuration and RRD files.

Recovery

site1 remains active. When you power on site2, site2 becomes standby. If you powered down or if the disaster recovery configuration is not deleted from site2, MySQL and PgSQL database replication and file transfer through SCP are initiated.

NOTE: When you rebuild or power on site2, if the disaster recovery configuration is deleted, you must reconfigure disaster recovery between both sites.

No Connectivity Between the Active Site (site1) and Arbiter Devices

Detection

The arbiterMonitor service of the disaster recovery watchdog at site1 detects that the percentage of reachable arbiter devices is below the configured warning threshold. An e-mail is sent to the administrator with this information.

Impact

There is no impact on the disaster recovery solution until the percentage of reachable arbiter devices goes below the failover threshold.

Recovery

No recovery is required because network management services are available from site1.

No Connectivity Between the Standby Site (site2) and Arbiter Devices

Detection

The arbiterMonitor service of the disaster recovery watchdog at site2 detects that the percentage of reachable arbiter devices is below the configured warning threshold. An e-mail is sent to the administrator with this information.

Impact

There is no impact on the disaster recovery solution.

Recovery

No recovery is required because network management services are available from site1.

RELATED DOCUMENTATION

- Disaster Recovery Overview | **1699**
- Modifying Applications and Nodes on a Disaster Recovery Setup | **1765**
- Manually Failing Over the Network Management Services to the Standby Site | **1780**
- Understanding High-Availability Failover Scenarios | **1687**

Understanding How the Standby Site Becomes Operational When the Active Site Goes Down

When a disaster causes the active site to go down, if automatic failover is enabled and the standby site can exceed the failure threshold, the standby site becomes operational. Otherwise, you may need to execute the **jmp-dr manualFailover** or **jmp-dr manualFailover –a** command at the standby site to resume network management services.

The disaster recovery watchdog at the standby site performs the following failover operations to become an active site:

- Verify that the VIP address at the active site is not reachable.
- Stop database replication and SCP file transfer between the two sites.
- Remove the cron job from the standby site for fetching backup files from the active site.
- Add a cron job at the standby site to back up configuration and RRD files.
- Modify the role of the standby site to active.
- Open port 7804 on all nodes at the standby site.
- Start all services at the standby site.
- Copy system configuration files contained in the backup to appropriate locations.
- Configure all devices to send SNMP traps to the VIP address of the standby site. If eth3 is used for device management at the standby site, the eth3 IP address of the active-VIP node at the standby site is configured as the trap destination, instead of the VIP address.

  If you are monitoring devices through a dedicated FMPM node, the VIP address of the dedicated node is configured as the trap destination.

After the failover is complete, the disaster recovery role of the site is set to Active and the state of the cluster is set to active (1). You can access the GUI and API of the standby site from its VIP to perform all network management tasks. In most cases, the failover should happen within 20 to 30 minutes. When the active site becomes operational again, it becomes the standby site. You can either retain the failed state or choose to revert to the original state.

RELATED DOCUMENTATION

Disaster Recovery Overview | **1699**

Understanding the Normal Operation of Active and Standby Sites | **1723**

Configuring the Disaster Recovery Process Between an Active and a Standby Site | **1731**

Understanding High-Availability Failover Scenarios | **1687**

CHAPTER 98

Configuring the Disaster Recovery Process

IN THIS CHAPTER

- Configuring the Disaster Recovery Process Between an Active and a Standby Site | 1731
- Stopping the Disaster Recovery Process on Junos Space Network Management Platform Release 14.1R3 and Earlier | 1743

Configuring the Disaster Recovery Process Between an Active and a Standby Site

IN THIS SECTION

- Configuring Disaster Recovery at the Active Site | 1732
- Configuring Disaster Recovery at the Standby Site | 1737
- Starting the Disaster Recovery Process | 1741
- Verifying the Status of the Disaster Recovery Process | 1743

You configure disaster recovery between an active site and a standby site to ensure geographical redundancy of network management services.

Before you initiate the disaster recovery process between both sites, perform the following tasks:

- Ensure that the connectivity requirements as described in the "Disaster Recovery Overview" on page 1699 topic are met.
- Check whether identical cluster configurations exist on both sites. We recommend that both clusters have the same number of nodes so that, even in the case of a disaster, the standby site can operate with the same capacity as the active site.
- Ensure that the same versions of Junos Space Network Management Platform, high-level Junos Space applications, and device adapters are installed at both sites.

- Shut down the disaster recovery process configured on Junos Space Network Management Platform Release 14.1R3 and earlier before upgrading to Junos Space Network Management Platform Release 15.2R1 and configuring the new disaster recovery process. For more information, see "Stopping the Disaster Recovery Process on Junos Space Network Management Platform Release 14.1R3 and Earlier" on page 1743.

  You cannot configure the new disaster recovery process if you do not stop the disaster recovery you set up on 14.1R3 and earlier releases. You do not need to perform this step on a clean installation of Junos Space Network Management Platform Release 15.2R1.

- Ensure that the same SMTP server configuration exists on both sites to receive e-mail alerts related to the disaster recovery process. You can add SMTP servers from the SMTP Servers task group in the Administration workspace. For more information about adding SMTP servers, see "Adding an SMTP Server" on page 1478 in the *Junos Space Network Management Platform Workspaces Feature Guide*.

- Copy a file with the list of arbitrator devices (one IP address per row) in the CSV format or the custom failure-detection scripts on the VIP node at the active site. You can refer to the sample files at **/var/cache/jmp-geo/doc/samples/**.

- Decide on the values for the following parameters depending on your network connectivity and disaster recovery requirements:

  - VIP address and password of both the active and standby sites
  - Backup, restoration, and Secure Copy Protocol (SCP) synchronization settings
  - Heartbeat time intervals
  - E-mail address of the administrator and the dampening interval in seconds to avoid reporting the same errors to avoid an e-mail flood
  - Failure-detection settings such as the failover threshold and the time during which the standby site stays standby if the arbiter devices are unreachable

The following sections explain how to configure disaster recovery at the active and standby sites and initiate the disaster recovery between both sites.

Configuring Disaster Recovery at the Active Site

You use the **jmp-dr init –a** command to configure disaster recovery at the active site. You need to enter values for the parameters that are displayed. The values you enter here are saved in a configuration file.

To configure disaster recovery at the active site:

1. Log in to the CLI of the Junos Space node at the active site on which the VIP or the eth0:0 interface is configured.

   The Junos Space Settings Menu is displayed.

2. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   The following is a sample output from a virtual appliance:

```
admin@10.206.41.183's password:
Last login: Mon Aug 17 06:17:58 2015 from 10.206.41.42

Welcome to the Junos Space network settings utility.

Initializing, please wait


Junos Space Settings Menu

1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> Expand VM Drive Size
7> (Debug) run shell

A> Apply changes
Q> Quit
R> Redraw Menu

Choice [1-7,AQR]: 7
```

   You are prompted to enter the administrator password.

3. Enter the administrator password.

4. Enter **jmp-dr init –a** at the shell prompt.

   The values you need to input to configure disaster recovery at the active site are displayed.

   The Load Balancers part of the disaster recovery configuration file is displayed.

5. Enter the values for the parameters displayed:
   a. Enter the VIP address of the standby site and press Enter.

   b. Enter the administrator passwords of the load-balancer nodes at the standby site and press Enter.

      You can enter multiple passwords separated with commas.

      If multiple nodes use a common password, you need to enter the password only once.

   c. Enter the timeout value to detect a failure in transferring files through SCP from the active site to the standby site, in seconds, and press Enter.

      The minimum and default value is 120.

   d. Enter the maximum number of backups to retain at the active site and press Enter.

      The minimum and default value is 3.

   e. Enter the times of the day to back up files (in hours) at the active site, separated with commas, and press Enter.

      You can enter any value from 0 through 23. You can also enter * to back up files every hour.

   f. Enter the days of the week to back up files at the active site, separated with commas, and press Enter.

      You can enter any value from 0 through 6, where Sunday equals zero. You can also enter * to back up files every day.

   g. Enter the times of the day to copy files (in hours) from the active site to the standby site, separated with commas, and press Enter.

      You can enter any value from 0 through 23. You can also enter * to poll files every hour.

   h. Enter the days of the week to copy files from the active site to the standby site, separated with commas, and press Enter.

      You can enter any value from 0 through 6, where Sunday equals zero. You can also enter * to poll files every day.

   The following is a sample output:

```
########################
#
# Load Balancers
```

```
#
#########################

What's the vip for load balancers at the standby site? 10.206.41.225
What are the unique admin passwords for load balancer nodes at the standby site
 (separated by comma, no space)? $ABC123
What's the scp timeout value (seconds)? 120

# backup for data in file system instead of DB

What's the max number of backup files to keep? 3
What are the times of the day to run file backup (0-23)?
0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23
What are the days of the week to run file backup (0-6)? 0,1,2,3,4,5,6

# restore for data in file system instead of DB

What are the times of the day to poll files from the active site (0-23)?
0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23
What are the days of the week to poll files from the active site (0-6)?
0,1,2,3,4,5,6
```

When you enter the values for all parameters, the DR Watchdog part of the disaster recovery configuration file is displayed.

6. Enter values for the parameters displayed:
   a. Enter the number of times the active site should send heartbeat messages to the standby site through ping after a heartbeat message times out and press Enter.

      The minimum and default value is 4.

   b. Enter the timeout value of each heartbeat message, in seconds, and press Enter.

      The minimum and default value is 5.

   c. Enter the time interval between two consecutive heartbeat messages to the standby site, in seconds, and press Enter.

      The minimum and default value is 30.

   d. Enter the e-mail address of the administrator to whom e-mail messages about disaster recovery service issues must be sent and press Enter.

e. Enter the time interval during which the same issues are not reported through e-mail (dampening interval), in seconds, and press Enter.

   The default value is 3,600. The minimum value is 300.

f. Specify the failure-detection mechanism.

   If you intend to use a custom failure-detection script:

   - Enter **Yes** in the failureDetection section and press Enter.

   If you intend to use the device arbitration algorithm:

   i. Enter **No** in the failureDetection section and press Enter.

   ii. Enter the threshold percentage to trigger a failover to the standby site by using the device arbitration algorithm and press Enter.

   You can enter any value from 0 to 1. The default value is 0.5.

g. Enter the path of the file containing the arbiter devices or the custom failure-detection scripts and press Enter.

The following is a sample output:

```
#########################
#
# DR Watchdog
#
#########################


# heartbeat

What's the number of times to retry heartbeat message? 4
What's the timeout of each heartbeat message (seconds)? 5
What's the heartbeat message interval between sites (seconds)? 30

# notification

What's the contact email address of service issues? user1@example.com
What's the dampening interval between emails of affected services (seconds)?
300

# failureDetection
```

```
Do you want to use custom failure detection? No
What's the threshold percentage to trigger failover? 0.5
What's the arbiters list file (note: please refer to example in
/var/cache/jmp-geo/doc/samples/arbiters.list)? /home/admin/user1
Check status of DR remote site: up
Prepare /var/cache/jmp-geo/incoming
                        [ OK ]
Configure contact email
                        [ OK ]
Modify firewall for DR remote IPs
                        [ OK ]
Configure NTP
                        [ OK ]
Configure MySQL database
                        [ OK ]
Configure PostgreSQL database
                        [ OK ]
Copy files to DR slave
                        [ OK ]
Command completed.
```

When you have entered values for all parameters, disaster recovery is initialized at the active site.

Configuring Disaster Recovery at the Standby Site

You use the **jmp-dr init –s** command to configure disaster recovery at the standby site. You need to enter values for the parameters that are displayed. The values you enter here are saved in a configuration file. By default, the standby site uses the failure-detection mechanism you configured at the active site, values you entered for file backup and restoration, heartbeat, and notifications if the standby site becomes an active site.

To configure disaster recovery at the standby site:

1. Log in to the CLI of the Junos Space node at the standby site on which the VIP or the eth0:0 interface is configured.

   The Junos Space Settings Menu is displayed.

2. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   You are prompted to enter the administrator password.

3. Enter the administrator password.

4. Enter **jmp-dr init –s** at the shell prompt.

   The values you need to input to configure disaster recovery at the standby site are displayed.

   The Load Balancers part of the disaster recovery configuration file is displayed.

5. Enter the values for the parameters displayed:

   a. Enter the VIP address of the active site and press Enter.

   b. Enter the administrator passwords of the load-balancer nodes at the active site and press Enter.

      You can enter multiple passwords separated with commas.

      If multiple nodes use a common password, you need to enter the password only once.

   c. Enter the timeout value to detect a failure in transferring files through SCP from the standby site to the active site, in seconds, and press Enter.

      The minimum and default value is 120.

   d. Enter the maximum number of backups to retain at the standby site and press Enter.

      The minimum and default value is 3.

   e. Enter the times of the day to back up files (in hours) at the standby site, separated with commas, and press Enter.

      You can enter any value from 0 through 23. You can also enter * to back up files every hour.

   f. Enter the days of the week to back up files at the standby site, separated with commas, and press Enter.

      You can enter any value from 0 through 6, where Sunday equals zero. You can also enter * to back up files every day.

   g. Enter the times of the day to copy files (in hours) from the standby site to the active site (when failed over to the standby site), separated with commas, and press Enter.

      You can enter any value from 0 through 23. You can also enter * to restore files every hour.

   h. Enter the days of the week to copy files from the standby site to the active site (when failed over to the standby site), separated with commas, and press Enter.

      You can enter any value from 0 through 6, where Sunday equals zero. You can also enter * to restore files every day.

The following is a sample output:

```
#########################
#
# Load Balancers
#
#########################

What's the vip for load balancers at the active site? 10.206.41.220
What are the unique admin passwords for load balancer nodes at the active site
 (separated by comma, no space)? $ABC123
What's the scp timeout value (seconds)? 120

# backup for data in file system instead of DB

What's the max number of backup files to keep? 3
What are the times of the day to run file backup (0-23)?
0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23
What are the days of the week to run file backup (0-6)? 0,1,2,3,4,5,6

# restore for data in file system instead of DB

What are the times of the day to poll files from the active site (0-23)?
0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23
What are the days of the week to poll files from the active site (0-6)?
0,1,2,3,4,5,6
```

When you enter the values for all parameters, the DR Watchdog part of the disaster recovery configuration file is displayed.

6. Enter the values for the parameters displayed.
   a. Enter the number of times the standby site should send heartbeat messages to the active site through ping after a heartbeat message times out and press Enter.

      The minimum and default value is 4.

   b. Enter the timeout value for each heartbeat message, in seconds, and press Enter.

      The minimum and default value is 5.

   c. Enter the time interval between two consecutive heartbeat messages to the active site, in seconds, and press Enter.

      The minimum and default value is 30.

d. Enter the e-mail address of the administrator to whom e-mail messages about disaster recovery service issues must be sent and press Enter.

e. Enter the time during which the same issues are not reported through e-mail (dampening interval), in seconds, and press Enter.

   The default value is 3,600. The minimum value is 300.

The following is a sample output:

```
#########################
#
# DR Watchdog
#
#########################


# heartbeat

What's the number of times to retry heartbeat message? 4
What's the timeout of each heartbeat message (seconds)? 5
What's the heartbeat message interval between sites (seconds)? 30

# notification

What's the contact email address of service issues? user1@example.com
What's the dampening interval between emails of affected services (seconds)?
300
Check status of DR remote site: up
Load /var/cache/jmp-geo/incoming/init.properties
                        [ OK ]
Configure contact email
                        [ OK ]
Modify firewall for DR remote IPs
                        [ OK ]
Configure NTP
                        [ OK ]
Sync jmp-geo group
                        [ OK ]
Configure MySQL database
                        [ OK ]
Configure PostgreSQL database
                        [ OK ]
Command completed.
```

When you have entered values for all parameters, disaster recovery is initialized at the standby site.

Starting the Disaster Recovery Process

You use the **jmp-dr start** command to start the disaster recovery process at both sites. You can also use the **jmp-dr start-a** command to start the disaster recovery process on the active site and the **jmp-dr start-s** command to start the disaster recovery process on the standby site.

To start the disaster recovery process:

1. Log in to the CLI of the Junos Space node at the active site on which the VIP or the eth0:0 interface is configured.

   The Junos Space Settings Menu is displayed.

2. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   You are prompted to enter the administrator password.

3. Enter the administrator password.

4. Enter **jmp-dr start** at the shell prompt.

   The disaster recovery process is initiated on both sites.

   The following is a sample output at the active site:

```
[user1@host]# jmp-dr start
Stop dr-watchdog if it's running
                        [ OK ]
Check status of DR remote site: up
Check current DR role: active

INFO: => start DR at current site: active

Add device management IPs of DR remote site to up devices
                        [ OK ]
Setup MySQL replication: master-master
                        [ OK ]
Start MySQL dump
                        [ OK ]
Setup PostgreSQL replication
                        [ OK ]
Start file & RRD replication
                        [ OK ]
```

```
Open firewall for device traffic
                        [ OK ]
Start services(jboss,jboss-dc,etc.)
                        [ OK ]
Start dr-watchdog
                        [ OK ]
Copy files to DR slave site
                        [ OK ]
Update DR role of current site: active
                        [ OK ]

INFO: => start DR at DR remote site: standby

Stop dr-watchdog if it's running
                        [ OK ]
Check status of DR remote site: up
Check current DR role: standby
Load /var/cache/jmp-geo/incoming/start.properties
                        [ OK ]
Stop services(jboss,jboss-dc,etc.)
                        [ OK ]
Block firewall for device traffic
                        [ OK ]
Reset MySQL init script and stop replication
                        [ OK ]
Scp backup file from peer site: /var/cache/jmp-geo/data/db.gz
                        [ OK ]
Start MySQL restore
                        [ OK ]
Setup MySQL replication and start replication
                        [ OK ]
Setup PostgreSQL replication
                        [ OK ]
Start files & RRD replication
                        [ OK ]
Start dr-watchdog
                        [ OK ]
Clean up /var/cache/jmp-geo/incoming
                        [ OK ]
Update DR role of current site: standby
                        [ OK ]
Command completed.
Command completed.
```

The disaster recovery process is initialized on the active site and the standby site.

Verifying the Status of the Disaster Recovery Process

We recommend that you execute the **jmp-dr health** command to verify the status (overall health) of the disaster recovery process at both the active and standby sites when you start the disaster recovery process on both sites. For more information about executing the **jmp-dr health** command, see "Checking the Status of the Disaster Recovery Configuration" on page 1747.

RELATED DOCUMENTATION

Disaster Recovery Overview | **1699**

Modifying the Disaster Recovery Configuration | **1754**

Modifying Applications and Nodes on a Disaster Recovery Setup | **1765**

Stopping the Disaster Recovery Process on Junos Space Network Management Platform Release 14.1R3 and Earlier

IN THIS SECTION

- Stopping the Backup Process at the Active Site | **1743**
- Stopping Collecting Backups from the Active Site | **1745**

To configure the disaster recovery enhancements added as part of the Junos Space Network Management Platform Release 15.2R1, you must first disable the disaster recovery feature on your current Junos Space setup (Junos Space Network Management Platform Release 14.1R3 and earlier) before upgrading to Junos Space Network Management Platform Release 15.2R1. You must stop backups at the active site and the standby site must stop collecting backups from the active site. The scripts to stop the backup and restoration process configured during earlier releases are stored at **/opt/jmp-geo/backup/script/** and **/opt/jmp-geo/restore/script/**.

Stopping the Backup Process at the Active Site

Stopping the backup process at the active site removes the cron job and stops the backup operation from being performed.

To stop the backup process at the active site:

1. Log in to the CLI of the Junos Space node at the active site on which the VIP or the eth0:0 interface is configured.

   The Junos Space Settings Menu is displayed.

2. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   The following is a sample output from a virtual appliance:

```
admin@10.206.41.183's password:
Last login: Mon Aug 17 06:17:58 2015 from 10.206.41.42

Welcome to the Junos Space network settings utility.

Initializing, please wait


Junos Space Settings Menu

1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> Expand VM Drive Size
7> (Debug) run shell

A> Apply changes
Q> Quit
R> Redraw Menu

Choice [1-7,AQR]: 7
```

   You are prompted to enter the administrator password.

3. Enter the administrator password.

4. Type **/opt/jmp-geo/backup/script/./backup.sh stop** at the shell prompt and press Enter.

   The following is a sample output:

```
Demoting this cluster from the DR Master Cluster Role ...
update cluster state successful
Stoping backup cron job...
Stopping crond: [ OK ]
Starting crond: [ OK ]
```

The backup process at the active site is stopped.

Stopping Collecting Backups from the Active Site

Stopping the restoration process at the standby site removes the cron job and stops collecting backups from the active site.

To stop the restoration process at the standby site:

1. Log in to the CLI of the Junos Space node at the active site on which the VIP or the eth0:0 interface is configured.

   The Junos Space Settings Menu is displayed.

2. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   The following is a sample output from a virtual appliance:

```
admin@10.206.41.183's password:
Last login: Mon Aug 17 06:17:58 2015 from 10.206.41.42

Welcome to the Junos Space network settings utility.

Initializing, please wait


Junos Space Settings Menu

1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> Expand VM Drive Size
7> (Debug) run shell

A> Apply changes
```

```
Q> Quit
R> Redraw Menu

Choice [1-7,AQR]: 7
```

You are prompted to enter the administrator password.

3. Enter the administrator password.

4. Type **/opt/jmp-geo/restore/script/./restore.sh stopPoll** at the shell prompt and press Enter.

   The following is a sample output:

```
Stoping restore cron job...
Stopping crond: [ OK ]
Starting crond: [ OK ]
Demoting this cluster from the DR Slave Cluster Role ...
update cluster state successful
opening port 7804 on user1@host....
jmp-firewall is stopped. Skip reloading
<response>
<message
</message>
<status>SUCCESS</success>
</response>
```

The standby site stops collecting backups from the active site.

RELATED DOCUMENTATION

Disaster Recovery Overview | **1699**

Configuring the Disaster Recovery Process Between an Active and a Standby Site | **1731**

CHAPTER 99

Managing the Disaster Recovery Solution

IN THIS CHAPTER

- Checking the Status of the Disaster Recovery Configuration | 1747
- Viewing the Disaster Recovery Configuration and Status of Watchdog Services | 1752
- Modifying the Disaster Recovery Configuration | 1754
- Modifying Applications and Nodes on a Disaster Recovery Setup | 1765
- Manually Failing Over the Network Management Services to the Standby Site | 1780
- Stopping the Disaster Recovery Process | 1784
- Resetting the Disaster Recovery Configuration | 1786

Checking the Status of the Disaster Recovery Configuration

You check the status of the disaster recovery configuration:

- After starting the disaster recovery process to ensure that the disaster recovery configuration is accurate, files are being replicated, and the disaster recovery watchdog is monitoring the disaster recovery setup
- After stopping the disaster recovery process, to ensure that file replication and disaster recovery watchdog process have stopped

You execute the **jmp-dr health** command to check the status of the disaster recovery configuration. This command checks the status of asynchronous data replication, file transfer, and disaster recovery watchdog, and the role of clusters in the disaster recovery setup. Errors found during command execution are listed in the command output.

> **NOTE:** If you have already executed the **jmp-dr health** command and the execution is in progress, executing another **jmp-dr health** command can display incorrect output. The output from the **jmp-dr health** command also lists whether another instance of the command is being executed.

To check the status of the disaster recovery configuration at a site:

1. Log in to the CLI of the Junos Space node at the site on which the VIP or the eth0:0 interface is configured.

   The Junos Space Settings Menu is displayed.

2. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   The following is a sample output from a virtual appliance:

```
admin@10.206.41.183's password:
Last login: Mon Aug 17 06:17:58 2015 from 10.206.41.42

Welcome to the Junos Space network settings utility.

Initializing, please wait


Junos Space Settings Menu

1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> Expand VM Drive Size
7> (Debug) run shell

A> Apply changes
Q> Quit
R> Redraw Menu

Choice [1-7,AQR]: 7
```

   You are prompted to enter the administrator password.

3. Enter the administrator password.

4. Enter **jmp-dr health** at the shell prompt.

   Junos Space Platform checks the status (overall health) of the disaster recovery configuration at the site.

- The following is a sample output of the **jmp-dr health** command after you start the disaster recovery process and execute the command at the active site:

```
[user1@host]# jmp-dr health
The DR role of this site: active
The DR state of this site: started
The status of DR watchdog: ready
The status of DR remote site: up
Check admin password of DR remote site
                         [ OK ]
Check mysql ca and server certificates
                         [ OK ]
Check mysql replication users
                         [ OK ]
Check file replication: backup cron job should be added
                         [ OK ]
Check mysql replication:

   node (10.206.41.221, user1@host) and peer node of same site

   (10.206.41.222, user2@host) should be master-master
                [ OK ]
Check pgsql replication:

   Pgsql replication betwwen this node (10.206.41.221, user1@host) and peer
node of same site
   (10.206.41.222, user2@host) should be master-slave.
                [ OK ]
Services (jboss, jboss-dc, etc.) should be up
                         [ OK ]
DR watchdog should be up
                         [ OK ]
Command completed.
```

- The following is a sample output of the **jmp-dr health** command after you start the disaster recovery process and execute the command at the standby site:

```
[user3@host]# jmp-dr health
The DR role of this site: standby
The DR state of this site: started
The status of DR watchdog: ready
The status of DR remote site: up
Check admin password of DR remote site
```

```
                         [ OK ]
Check mysql ca and server certificates
                         [ OK ]
Check mysql replication users
                         [ OK ]
Check file replication: poll cron job should be added
                         [ OK ]
Check mysql replication:

   node (10.206.41.226, user3@host) and peer node of same site

   (10.206.41.227, user4@host) should be master-slave,

   and node (10.206.41.226, user3@host) and mysql VIP node of remote site

   (10.206.41.220) should be slave-master
                         [ OK ]
Check pgsql replication:

   Pgsql replication between node (10.206.41.226, user3@host) and peer node
of same site
   (10.206.41.227, user4@host) should be master-slave,

   and replication node (10.206.41.226, user3@host) and pgsql VIP node of
remote site
   (10.206.41.220) should be slave-master
                         [ OK ]
Services (jboss, jboss-dc, etc.) should be down
                         [ OK ]
DR watchdog should be up
                         [-]
 [ OK ]
Command completed.
```

- The following is a sample output of the **jmp-dr health** command after you stop the disaster recovery process and execute the command at the active site:

```
[user2@host]# jmp-dr health
The DR role of this site: active
The DR state of this site: stopped
The status of DR watchdog: ready
The status of DR remote site: up
Check admin password of DR remote site
```

```
                          [ OK ]
Check mysql ca and server certificates
                          [ OK ]
Check mysql replication users
                          [ OK ]
Check file replication: cron jobs should be removed
                          [ OK ]
Check mysql replication:

   node (10.206.41.222, user2@host) and peer node of same site

   (10.206.41.221, user1@host) should be master-master
                  [ OK ]
Services (jboss, jboss-dc, etc.) should be up
                          [ OK ]
DR watchdog should be down
                          [ OK ]
Command completed.
```

- The following is a sample output of the **jmp-dr health** command after you stop the disaster recovery process and execute the command at the standby site:

```
[user3@host]# jmp-dr health
The DR role of this site: standby
The DR state of this site: stopped
The status of DR watchdog: ready
The status of DR remote site: up
Check admin password of DR remote site
                          [ OK ]
Check mysql ca and server certificates
                          [ OK ]
Check mysql replication users
                          [ OK ]
Check file replication: cron jobs should be removed
                          [ OK ]
Check mysql replication:

   node (10.206.41.226, user3@host) and peer node of same site

   (10.206.41.227, user4@host) should be master-master
                  [ OK ]
Services (jboss, jboss-dc, etc.) should be down
                          [ OK ]
```

```
DR watchdog should be down
                          [ OK ]
Command completed.
```

RELATED DOCUMENTATION

- Configuring the Disaster Recovery Process Between an Active and a Standby Site | 1731
- Resetting the Disaster Recovery Configuration | 1786
- Stopping the Disaster Recovery Process | 1784

Viewing the Disaster Recovery Configuration and Status of Watchdog Services

You execute the **jmp-dr api v1 config** command to view the disaster recovery configuration and the status of the disaster recovery watchdog services at the local site. You can use this command to create custom failure-detection scripts. For more information about using custom failure-detection scripts, see the *Failure Detection by Using Custom Failure-Detection Scripts* section in the "Disaster Recovery Overview" on page 1699 topic. You can also refer to the sample scripts located at **var/cache/jmp-geo/doc/samples/**.

To view the disaster recovery configuration and the status of the disaster recovery watchdog services:

1. Log in to the CLI of the Junos Space node at the site on which the VIP or the eth0:0 interface is configured.

   The Junos Space Settings Menu is displayed.

2. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   The following is a sample output from a virtual appliance:

```
admin@10.206.41.183's password:
Last login: Mon Aug 17 06:17:58 2015 from 10.206.41.42

Welcome to the Junos Space network settings utility.

Initializing, please wait
```

```
Junos Space Settings Menu

1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> Expand VM Drive Size
7> (Debug) run shell

A> Apply changes
Q> Quit
R> Redraw Menu

Choice [1-7,AQR]: 7
```

You are prompted to enter the administrator password.

3. Enter the administrator password.

4. Enter **jmp-dr api v1 config** at the shell prompt.

   You can view the disaster recovery configuration and the status of all the disaster recovery watchdog services.

5. (Optional) To view the sections of the disaster recovery configuration, enter **jmp-dr api v1 config --list** at the shell prompt.

   All available sections of the disaster recovery configuration from the remote site are displayed.

   The following is a sample output:

```
[user1@host]# jmp-dr api v1 config --list
{
  "sections":
"role,failover,states,core,mysql,psql,file,watchdog,deviceManagement"
}
```

6. (Optional) To view selected sections of the disaster recovery configuration, enter **jmp-dr api v1 config --include <section1>,<section2>** at the shell prompt.

   The following is a sample output of the core and deviceManagement sections:

```
[user1@host]# jmp-dr api v1 config --include core,deviceManagement
{
  "core": {
    "peerVip": "10.206.41.41",
    "adminPass":
"53616c7465645f5f737061636531323312 6c3f3e6fd6257a81cded28f55d465c",
    "scpTimeout": 120,
    "peerLoadBalancerNodes": "10.206.41.42,10.206.41.44",
    "peerBusinessLogicNodes": "10.206.41.42,10.206.41.44,10.206.41.50",
    "peerDeviceMgtIps": "10.206.41.42,10.206.41.44,10.206.41.50"
  },
  "deviceManagement": {
    "peerNodes": "10.206.41.42,10.206.41.44,10.206.41.50",
    "nodes": "10.206.41.182,10.206.41.183,10.206.41.184",
    "ip": "10.206.41.183,eth0"
  }
}
```

RELATED DOCUMENTATION

Configuring the Disaster Recovery Process Between an Active and a Standby Site | 1731

Checking the Status of the Disaster Recovery Configuration | 1747

Stopping the Disaster Recovery Process | 1784

Modifying the Disaster Recovery Configuration

After you have initially configured the disaster recovery setup, you may need to modify the Junos Space cluster at either sites such as addition or removal of nodes from your Junos Space setup, change IP addresses of interfaces, change device management interfaces, load balancer details (VIP address and password), and change VIP address of dedicated services such as FMPM or database. You may also need to modify disaster recovery parameters such as backup and restore settings, heartbeat settings, and failure detection settings.

You use the **jmp-dr toolkit config update** command to:

- Reinitiate MySQL or PgSQL replication at a site and to the standby site if you added or removed dedicated nodes and update these changes at the standby site.
- Update the changes in cluster configuration (addition or removal of load balancer nodes), at both sites.

Refer to "Modifying Applications and Nodes on a Disaster Recovery Setup" on page 1765 for more information about modifying nodes.

You use the options along with **jmp-dr toolkit config update** command to modify backup and restore settings, heartbeat settings, failure detection settings, update load balancer details (VIP address and password), and SCP timeout settings, and update these changes at the peer site.

> **NOTE:** You must update the changes to the load balancers at both sites by using the **--user-core** option before modifying and updating the other sections of disaster recovery such as heartbeat settings, notification settings, failure detection settings, file backup and restore settings.

Table 210 lists the options and the group of disaster recovery configuration parameters included with the option.

Table 210: jmp-dr toolkit config update command options

Configuration Update Option	Description
--user-core	Load balancer VIP and password, and SCP timeout settings
--user-file-backup	Configuration and RRD files backup settings
--user-file-restore	Configuration and RRD files replication to standby site settings
--user-watchdog-heartbeat	Watchdog heartbeat settings
--user-watchdog-notification	Email notification settings
--user-watchdog-failureDetection	Failure detection settings

To modify the disaster recovery configuration:

1. Log in to the CLI of the Junos Space node at the active site on which the VIP or the eth0:0 interface is configured.

   The Junos Space Settings Menu is displayed.

2. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   The following is a sample output from a virtual appliance:

```
admin@10.206.41.183's password:
Last login: Mon Aug 17 06:17:58 2015 from 10.206.41.42

Welcome to the Junos Space network settings utility.

Initializing, please wait


Junos Space Settings Menu

1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> Expand VM Drive Size
7> (Debug) run shell

A> Apply changes
Q> Quit
R> Redraw Menu

Choice [1-7,AQR]: 7
```

3. Enter the administrator password.

4. Stop the disaster recovery process on both sites. To do so, type **jmp-dr stop** at the shell prompt and press Enter.

5. Perform the following steps to modify the disaster recovery configuration at sites.

- Use the **jmp-dr toolkit config update** command to:
  - Update the addition or removal of load balancer nodes.
  - Reinitiate MySQL or PgSQL replication at a site (after adding or removing dedicated nodes).
  - Update changes to VIP address of FMPM node or database node of a site, at both sites.
  - Update the changes to IP address of the nodes of a site, at both sites.
  - Update the addition or removal of eth3 interface for device management or change in the IP address of the eth3 interface, at both sites.
  - Update the change of IP address version for device management (IPv4 to IPv6 or IPv6 to IPv4) of a site, at both sites.

  a. Log in to the CLI of the Junos Space VIP node at the site where you made the modifications.

  b. Type **jmp-dr toolkit config update** at the shell prompt and press Enter.

  c. Type No and press Enter to view the cluster modifications.

     The modified cluster configuration is displayed in JSON format.

  d. Press Enter to accept the changes.

     The following is a sample output when the disaster recovery configuration is updated after adding a dedicated MySQL node.

```
[user1@host]# jmp-dr toolkit config update
If admin password of any node belonging to remote site is changed or if a
new node with different admin password is added then please use option
--user-core. Continue? Yes
The modified user configuration in JSON format is as follows:
{
  "user_mysql_hasDedicatedDb": {
    "lhs": false,
    "rhs": true
  },
  "user_mysql_peerVip": {
    "lhs": "10.206.41.225",
    "rhs": "10.206.41.84"
  },
  "user_mysql_peerNodes": {
    "lhs": "10.206.41.226,10.206.41.227",
    "rhs": "10.206.41.85,10.206.41.86"
  }
}
```

```
Do you want to apply these changes? Yes
Check status of DR remote site: up
Stop mysql replication if applicable
                            [ OK ]
Update mysql repUser & repAdmin
                            [ OK ]
Update firewall
                            [ OK ]
Update ntp
                            [ OK ]
Update mysql configuration if applicable
                            [ OK ]
Update services (such as jboss-dc, httpd, etc.)
                            [ OK ]
The configuration change is updated only at current site, please ensure to
 update at the remote site accordingly.
The `toolkit config` command is done
```

The disaster recovery configuration file at the local site is updated with the modified configuration of the cluster.

e. Log in to the CLI of the Junos Space VIP node at the peer site to update the modifications made at the local site.

f. Type **jmp-dr toolkit config update** at the shell prompt and press Enter.

g. Type No and press Enter to view the modified cluster configuration at the remote site.

The modified configuration is displayed in JSON format.

h. Press Enter to accept the changes.

The disaster recovery configuration file at the peer site is updated with the modified configuration of the cluster at the local site.

- To modify the heartbeat settings at a site:

a. Log in to the CLI of the Junos Space VIP node at the site where the heartbeat settings must be modified.

b. Type **jmp-dr toolkit config update --user-watchdog-heartbeat** at the shell prompt and press Enter.

c. Type No and press Enter to modify the heartbeat settings.

The disaster recovery configuration parameters to modify heartbeat settings are displayed.

The following is a sample screen output.

```
? If admin password of any node belonging to remote site is changed or if
a new node with different admin password is added then please use option
--user-core. Continue? Yes

#########################
#
# DR Watchdog
#
#########################


# heartbeat

? What's the number of times to retry heartbeat message? 4
? What's the timeout of each heartbeat message (seconds)? 5
? What's the heartbeat message interval between sites (seconds)? 30
```

d. Modify the heartbeat settings.

   The modified heartbeat settings are displayed in JSON format.

e. Press Enter to accept the changes.

   The heartbeat settings are modified when the command is executed.

   The following is a sample screen output.

```
The configuration change is updated only at current site, please ensure to
 update at the remote site accordingly.
Command completed.
```

f. Log in to the CLI of the Junos Space VIP node at the peer site to update the modifications made at the local site.

g. Type **jmp-dr toolkit config update --user-watchdog-heartbeat** at the shell prompt and press Enter.

h. Type No and press Enter to view the modified heartbeat settings at the local site.

   The modified heartbeat settings are displayed in JSON format.

i. Press Enter to accept the changes.

The heartbeat settings are updated when the command is executed.

- To modify the notification settings at a site:

  a. Log in to the CLI of the Junos Space VIP node at the site where the notification settings must be modified.

  b. Type **jmp-dr toolkit config update --user-watchdog-notification** at the shell prompt and press Enter.

  c. Type No and press Enter to modify the notification settings.

     The disaster recovery configuration parameters to modify notification settings are displayed.

  d. Modify the notification settings.

     The modified notification settings are displayed in JSON format.

  e. Press Enter to accept the changes.

     The notification settings are modified when the command is executed.

  f. Log in to the CLI of the Junos Space VIP node at the peer site to update the modifications made at the local site.

  g. Type **jmp-dr toolkit config update --user-watchdog-notification** at the shell prompt and press Enter.

  h. Type No and press Enter to view the modified notification settings at the local site.

     The modified notification settings are displayed in JSON format.

  i. Press Enter to accept the changes.

     The notification settings are updated when the command is executed.

- To modify the failure detection settings at the active site:

  a. Log in to the CLI of the Junos Space VIP node at the active site.

  b. Type **jmp-dr toolkit config update --user-watchdog-failureDetection** at the shell prompt and press Enter.

  c. Type No and press Enter to modify the failure detection settings.

     The disaster recovery configuration parameters to modify failure detection settings are displayed.

d. Modify the failure detection settings.

   The modified failure detection settings are displayed in JSON format.

e. Press Enter to accept the changes.

   The failure detection settings are modified when the command is executed.

   The following is a sample screen output.

```
? If admin password of any node belonging to remote site is changed or if
a new node with different admin password is added then please use option
--user-core. Continue? Yes

#########################
#
# DR Watchdog
#
#########################


# failureDetection

? Do you want to use custom failure detection? No
? What's the threshold percentage to trigger failover? 50
? What's the arbiters list file (note: please refer to example in
/var/cache/jmp-geo/doc/samples/arbiters.list)?
/var/cache/jmp-geo/doc/arbiters.list
The modified user configuration in JSON format is as follows:
{
  "user_watchdog_failureDetection_arbiters": {
    "lhs": "/var/cache/jmp-geo/config/arbiters.list",
    "rhs": "/var/cache/jmp-geo/doc/arbiters.list"
  }
}

? Do you want to apply these changes? Yes
Check status of DR remote site: up
Update MySQL configuration if applicable
                             [ OK ]
Update services (such as jboss-dc, httpd, etc.)
                             [ OK ]
The configuration change is updated only at current site, please ensure to
 update at the remote site accordingly.
Command completed.
```

f. Log in to the CLI of the Junos Space VIP node at the peer site to update the modifications made at the active site.

g. Type **jmp-dr toolkit config update --user-watchdog-failureDetection** at the shell prompt and press Enter.

h. Type No and press Enter to view the modified failure detection settings at the local site.

   The modified failure detection settings are displayed in JSON format.

i. Press Enter to accept the changes.

   The failure detection settings are updated when the command is executed.

- To modify the file backup settings at a site:

  a. Log in to the CLI of the Junos Space VIP node at the site where the file backup settings must be modified.

  b. Type **jmp-dr toolkit config update --user-file-backup** at the shell prompt and press Enter.

  c. Type No and press Enter to modify the file backup settings.

     The disaster recovery configuration parameters to modify file backup settings are displayed.

  d. Modify the file backup settings.

     The modified file backup settings are displayed in JSON format.

  e. Press Enter to accept the changes.

     The file backup settings are modified when the command is executed.

  f. Log in to the CLI of the Junos Space VIP node at the peer site to update the modifications made at the local site.

  g. Type **jmp-dr toolkit config update --user-file-backup** at the shell prompt and press Enter.

  h. Type No and press Enter to view the modified file backup settings at the local site.

     The modified file backup settings are displayed in JSON format.

  i. Press Enter to accept the changes.

     The file backup settings are updated when the command is executed.

- To modify the file restore settings at a site:

  a. Log in to the CLI of the Junos Space VIP node at the site where the file restore settings must be modified.

  b. Type **jmp-dr toolkit config update --user-file-restore** at the shell prompt and press Enter.

  c. Type No and press Enter to modify the file restore settings.

     The disaster recovery configuration parameters to modify file restore settings are displayed.

  d. Modify the file restore settings.

     The modified file restore settings are displayed in JSON format.

  e. Press Enter to accept the changes.

     The file restore settings are modified when the command is executed.

  f. Log in to the CLI of the Junos Space VIP node at the peer site to update the modifications made at the local site.

  g. Type **jmp-dr toolkit config update --user-file-restore** at the shell prompt and press Enter.

  h. Type No and press Enter to view the modified file restore settings at the local site.

     The modified file restore settings are displayed in JSON format.

  i. Press Enter to accept the changes.

The file restore settings are updated when the command is executed.

- Use the **--user-core** option to:
  - Update the modified VIP address of the load balancers of a site at the peer site.
  - Update the modified password of the load balancers of the standby a site at the active site.

    NOTE: You can use the **--user-core** option to update the modified password of the active site at the standby site.

  Refer to "Modifying the Network Settings of a Node in the Junos Space Fabric" on page 1264 in the *Junos Space Network Management Platform Workspaces Feature Guide* for more information about modifying the VIP address of the load balancers.

  - Modify the SCP timeout settings at a site.

a. Log in to the CLI of the Junos Space VIP node at the site where the load balancer details are modified or where the SCP timeout settings must be modified.

b. Type **jmp-dr toolkit config update --user-core** at the shell prompt and press Enter.

c. Press Enter to update the load balancer modifications or modify the SCP timeout settings.

   The disaster recovery configuration parameters to modify load balancer settings are displayed.

d. Modify the load balancer settings.

   The modified load balancer settings are displayed in JSON format.

e. Press Enter to apply the changes.

   The load balancer settings are modified when the command is executed.

   The following is a sample screen output.

```
[user1@host]# jmp-dr toolkit config update --user-core

#########################
#
# Load Balancers
#
#########################

? What's the vip for load balancers at the standby site? 10.206.41.101
```

```
? What are the unique admin passwords for load balancer nodes at the standby
 site (separated by comma, no space)? $ABC123
? What's the scp timeout value (seconds)? 120
Check status of DR remote site: up
Update MySQL configuration if applicable
                            [ OK ]
Update services (such as jboss-dc, httpd, etc.)
                            [ OK ]
The configuration change is updated only at current site, please ensure to
 update at the remote site accordingly.
Command completed.
```

f. Log in to the CLI of the Junos Space VIP node at the peer site.

g. Type **jmp-dr toolkit config update --user-core** at the shell prompt and press Enter.

   The modified load balancer settings are displayed in JSON format.

h. Press Enter to accept the changes.

   The load balancer settings are modified when the command is executed.

6. Start the disaster recovery process on both sites from the active site. To do so, type **jmp-dr start** at the shell prompt and press Enter.

RELATED DOCUMENTATION

- Configuring the Disaster Recovery Process Between an Active and a Standby Site | **1731**
- Resetting the Disaster Recovery Configuration | **1786**
- Stopping the Disaster Recovery Process | **1784**

Modifying Applications and Nodes on a Disaster Recovery Setup

IN THIS SECTION

- Upgrading the Junos Space Network Management Platform Software | **1767**
- Upgrading to Junos Space Network Management Platform Release 16.1R1 | **1772**
- Installing a Junos Space Application | **1773**

- Upgrading a Junos Space Application | **1774**
- Uninstalling a Junos Space Application | **1775**
- Adding or Removing a JBoss Node | **1776**
- Adding or Removing a Dedicated Junos Space Node | **1778**

During routine operations of the disaster recovery setup, you may need to make changes to the disaster recovery setup such as upgrading Junos Space Network Management Platform; adding, removing, or upgrading Junos Space applications; adding nodes; and changing disaster recovery settings or disaster recovery procedures when the active site goes down due to a disaster. You need to log in to the Junos Space user interface and initiate Junos Space Platform workflows to modify the applications and nodes.

NOTE: You must stop the disaster recovery process when you make changes to the disaster recovery setup. Missing transactions at the standby site are collected from the active site when you restart the disaster recovery process after modifying the setup.

NOTE: We recommend that you install the same set of applications on both sites to ensure that you can use all the applications from the standby site in case of a failover.

NOTE: When you execute the scripts to install and upgrade Junos Space Platform and Junos Space applications, you must enter only the release version. For example, **/var/www/cgi-bin/executeUpgradeOnDr.pl *16.1R1.XX*** and not **/var/www/cgi-bin/executeUpgradeOnDr.pl *16.1R1.XX.img***.

When you execute disaster recovery scripts, ensure that you use only the following special characters to create user names and passwords:

Table 211: Supported Special Characters

Supported Special Characters
!
#

Table 211: Supported Special Characters ***(continued)***

%
*
–
-
=
+
[
{
]
}
;
,
.
/

The following sections contain steps to modify the applications or nodes on a disaster recovery setup.

Upgrading the Junos Space Network Management Platform Software

You upgrade Junos Space Platform at both the active and standby sites to upgrade the version of Junos Space Platform on your Junos Space deployment. You can upgrade Junos Space Platform on both sites as follows:

- Upgrade Junos Space Platform at the standby site before you upgrade Junos Space Platform at the active site. By upgrading the software image on the standby site first, you can verify the software upgrade process without impacting normal operations at the active site. Although you can upgrade the software on the standby site by using scripts, you must manually failover to the standby site to verify the functionality and features of Junos Space Platform from the user interface. By upgrading the software image on the standby site first, you also ensure that the new software and new database schema are

first made available on the standby site to enable it to receive new backup files from the active site after upgrading the software on the active site and restarting disaster recovery.

- Upgrade Junos Space Platform at the active site before you upgrade Junos Space Platform at the standby site. By upgrading and testing Junos Space Platform for a duration that allows no disaster recovery functionality on your Junos Space setup, and using the newer version of Junos Space Platform on the active site first, you ensure that all functionality and features accessible through the user interface work as expected. You can then upgrade the software on the standby site by using scripts or by manually failing over to the standby site and upgrading from the user interface.

You execute the **./executeScpImageOnDr.pl** and **./executeUpgradeOnDr.pl** scripts to upgrade Junos Space Platform Release to later releases. You need to stop the disaster recovery process on both sites before uploading and upgrading the software on both sites, reboot all nodes at both sites, and start the disaster recovery process from the active site.

> **NOTE:** See Table 211 for information about the usage of supported special characters to create user name and passwords, while executing disaster recovery scripts.

To upgrade Junos Space Platform to a later release:

> **NOTE:** If you are upgrading Junos Space Platform to Release 18.1 from a version earlier than Release 16.1, you must first upgrade Junos Space Platform to Release 16.1, and then upgrade Junos Space Platform Release 16.1 to Release 17.1 or Release 17.2.
>
> If you are upgrading to Junos Space Platform Release 16.1 from an earlier version, follow the steps listed in the "Upgrading to Junos Space Network Management Platform Release 16.1R1" on page 1772 section.

> **NOTE:** Before you upgrade Junos Space Platform to Release 18.1, ensure that the time on all Junos Space nodes is synchronized. For information about synchronizing time on Junos Space nodes, see Synchronizing Time Across Junos Space Nodes

1. Log in to the CLI of the Junos Space node at the active site on which the VIP or the eth0:0 interface is configured.

   The Junos Space Settings Menu is displayed.

2. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

The following is a sample output from a virtual appliance:

```
admin@10.206.41.183's password:
Last login: Mon Aug 17 06:17:58 2015 from 10.206.41.42

Welcome to the Junos Space network settings utility.

Initializing, please wait


Junos Space Settings Menu

1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> Expand VM Drive Size
7> (Debug) run shell

A> Apply changes
Q> Quit
R> Redraw Menu

Choice [1-7,AQR]: 7
```

You are prompted to enter the administrator password.

3. Enter the administrator password.

4. You can start upgrading the software at the active site or the standby site.

   To upgrade the active site first:

   a. Stop the disaster recovery process on both sites. To do so, type **jmp-dr stop** at the shell prompt of the active site and press Enter.

   b. Go to the Junos Space user interface > Administration workspace > Applications page and upload the software image to the active site. The software image file should be listed on the Upgrade Platform page. Refer to “Upgrading Junos Space Network Management Platform” on page 1378 in the *Junos Space Network Management Platform Workspaces Feature Guide*.

c. Use SCP to copy the software image from the active site to the standby site. To do so, type **/var/www/cgi-bin/executeScpImageOnDr.pl *software-image-name*** at the shell prompt at the active site and press Enter.

   The software image is copied from the **/var/cache/jboss/jmp/** directory at the active site to the **/var/cache/jboss/jmp/payloads/** directory at the standby site.

d. Go to the Junos Space user interface > Administration workspace > Applications page and upgrade the software at the active site. Refer to "Upgrading Junos Space Network Management Platform" on page 1378 in the *Junos Space Network Management Platform Workspaces Feature Guide*.

e. When the upgrade is complete and all nodes reboot, check the functionality of Junos Space Platform from the user interface.

f. Upgrade the software on the standby site. To do so, type **/var/www/cgi-bin/executeUpgradeOnDr.pl *software-image-name*** at the shell prompt at the active site and press Enter.

g. Verify that the software is upgraded at the standby site as follows:

   - Verify from the log entry in the **install.log** file located at **/var/log/**.
   - Execute the **rpm -qa | grep jmp-** command and verify that the following RPMs are upgraded: **Jmp-nma**, **Jmp-cmp**, **jmp-ems**, and other **jmp**-related RPMs.

h. Reboot all nodes at the standby site from the CLI. To do so, type **reboot** at the shell prompt of each node and press Enter.

i. Since the standby site cannot be accessed through the user interface, you must manually failover to the standby site to access the user interface. To do so, type **jmp-dr manualFailover** at the shell prompt of the standby site and press Enter.

j. Verify the functionality of Junos Space Platform on the standby site.

k. Manually failover to the original active site. To do so, type **jmp-dr manualFailover** at the shell prompt of the current standby site and press Enter.

l. Start the disaster recovery process on both sites from the active site. To do so, type **jmp-dr start** at the shell prompt and press Enter.

To upgrade the standby site first:

a. Since the standby site cannot be accessed through the user interface, you must manually failover to the standby site to access the user interface on the standby site and upgrade the software. To do so, type **jmp-dr manualFailover** at the shell prompt of the standby site and press Enter.

   The standby site is the new active site. From steps b through j the original active site is referred as the standby site and the original standby site is referred as the active site.

b. Stop the disaster recovery process on both sites. To do so, type **jmp-dr stop** at the shell prompt of the active site and press Enter.

c. Go to the Junos Space user interface > Administration workspace > Applications page and upload the software image to the active site. The software image file should be listed on the Upgrade Platform page. Refer to "Upgrading Junos Space Network Management Platform" on page 1378 in the *Junos Space Network Management Platform Workspaces Feature Guide*.

d. Use SCP to copy the software image from the active site to the standby site. To do so, type **/var/www/cgi-bin/executeScpImageOnDr.pl *software-image-name*** at the shell prompt at the active site and press Enter.

   The software image is copied from the **/var/cache/jboss/jmp/** directory at the active site to the **/var/cache/jboss/jmp/payloads/** directory at the standby site.

e. Go to the Junos Space user interface > Administration workspace > Applications page and upgrade the software at the active site. Refer to "Upgrading Junos Space Network Management Platform" on page 1378 in the *Junos Space Network Management Platform Workspaces Feature Guide*.

f. When the upgrade is complete and all nodes reboot, check the functionality of Junos Space Platform from the user interface.

g. Upgrade the software on the standby site. To do so, type **/var/www/cgi-bin/executeUpgradeOnDr.pl *software-image-name*** at the shell prompt at the active site and press Enter.

h. Verify that the software is upgraded at the standby site as follows:

   - Verify from the log entry in the **install.log** file located at **/var/log/**.

- Execute the **rpm -qa | grep jmp-** command and verify that the following RPMs are upgraded: **Jmp-nma**, **Jmp-cmp**, **jmp-ems**, and other **jmp**-related RPMs.

i. Reboot all nodes at the standby site from the CLI. To do so, type **reboot** at the shell prompt of each node and press Enter.

j. Since the standby site cannot be accessed through the user interface, you must manually failover to the standby site (the original active site at the start of the upgrade process) to access the user interface. To do so, type **jmp-dr manualFailover** at the shell prompt of the original active site and press Enter.

   The

k. Verify the functionality of Junos Space Platform on the active site.

l. Start the disaster recovery process on both sites from the active site. To do so, type **jmp-dr start** at the shell prompt and press Enter.

Junos Space Platform is upgraded on the active and standby sites.

> **NOTE:** We recommend that you execute the **jmp-dr health** command at both sites and verify the output after starting disaster recovery on the upgraded setup.

Upgrading to Junos Space Network Management Platform Release 16.1R1

You can upgrade to Junos Space Network Management Platform Release 16.1R1 only from Junos Space Platform Release 15.2R2. To upgrade to Junos Space Platform Release 16.1R1 from releases prior to Junos Space Platform Release 15.2R2, you must first upgrade Junos Space Platform to Junos Space Platform Release 15.2R2. For more information about upgrading to Junos Space Platform Release 15.2R2, refer to the Junos Space Network Management Platform Release 15.2R2 Release Notes.

In Junos Space Platform Release 16.1R1, CentOS 6.8 is used as the underlying OS. A direct upgrade of the OS from CentOS 5.9 to CentOS 6.8 is not recommended, therefore, a direct upgrade to Junos Space Platform Release 16.1R1 by using the Junos Space Platform UI is not supported. You must follow a multi-step procedure to upgrade to Junos Space Platform Release 16.1R1.

To upgrade to Junos Space Platform Release 16.1R1 on a setup that has disaster recovery configured, you must upgrade both the active and standby sites by following the procedure outlined in Upgrading to Junos Space Network Management Platform Release 16.1R1 and then reconfigure disaster recovery. For more information about configuring disaster recovery, see “Configuring the Disaster Recovery Process Between an Active and a Standby Site” on page 1731.

Installing a Junos Space Application

You install a Junos Space application on both sites to add the application to your Junos Space deployment. You execute the **./executeScpImageOnDr.pl** and **./executeInstallAppOnDr.pl** scripts to install an application.

> **NOTE:** See Table 211 for information about the usage of supported special characters to create user name and passwords, while executing disaster recovery scripts.

To install a Junos Space application on both sites:

1. Log in to the CLI of the Junos Space node at the active site on which the VIP or the eth0:0 interface is configured.

   The Junos Space Settings Menu is displayed.

2. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   You are prompted to enter the administrator password.

3. Enter the administrator password.

4. Stop the disaster recovery process on both sites. To do so, type **jmp-dr stop** at the shell prompt and press Enter.

5. Go to the Junos Space user interface > Administration workspace > Applications page to upload the application image to the active site. Refer to the Adding a Junos Space Application workflow in the *Junos Space Network Management Platform Workspaces Feature Guide*.

6. Use SCP to copy the application image to the standby site from the active site. To do so, type **/var/www/cgi-bin/./executeScpImageOnDr.pl *application-image-name*** at the shell prompt at the active site and press Enter.

   The application image is copied from the **/var/cache/jboss/jmp/** directory at the active site to the **/var/cache/jboss/jmp/payloads/** directory at the standby site.

7. Go to the Junos Space user interface > Administration workspace > Applications page to install the application on the active site. Refer to "Adding a Junos Space Application" on page 1372 in the *Junos Space Network Management Platform Workspaces Feature Guide*.

8. Go to the Junos Space user interface > Job Management page to verify that the application is installed on the active site.

9. Install the application image on the standby site. To do so, type **/var/www/cgi-bin/./executeInstallAppOnDr.pl** ***application-image-name*** at the shell prompt at the active site and press Enter.

10. Verify the following on the standby site:
    - RPMs of the application are installed. To verify, execute the following command: **rpm -qa | grep <application-rpm-name>**.
    - **.ear** files of the application are available at **/usr/local/jboss/standalone/deployments/**.
11. Start the disaster recovery process on both sites from the active site. To do so, type **jmp-dr start** at the shell prompt of the VIP node at the active site and press Enter.

The Junos Space application is installed on the active and standby sites.

Upgrading a Junos Space Application

You upgrade a Junos Space application on both sites to upgrade the application on your Junos Space deployment. You execute the **./executeScpImageOnDr.pl** and **./executeInstallAppOnDr.pl** scripts to upgrade a Junos Space application.

To upgrade a Junos Space application on both sites:

1. Log in to the CLI of the Junos Space node at the active site on which the VIP or the eth0:0 interface is configured.

   The Junos Space Settings Menu is displayed.

2. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   You are prompted to enter the administrator password.

3. Enter the administrator password.

4. Stop the disaster recovery process on both sites. To do so, type **jmp-dr stop** at the shell prompt and press Enter.

5. Go to the Junos Space user interface > Administration workspace > Applications page to upload the application image to the active site. Refer to the Upgrading a Junos Space Application workflow in the *Junos Space Network Management Platform Workspaces Feature Guide*.

6. Use SCP to copy the application image to the standby site from the active site. To do so, type **/var/www/cgi-bin/./executeScpImageOnDr.pl *application-image-name*** at the shell prompt at the active site and press Enter.

7. Go to the Junos Space user interface > Administration workspace > Applications page to upgrade the application on the active site. Refer to "Upgrading a Junos Space Application" on page 1376 in the *Junos Space Network Management Platform Workspaces Feature Guide*.

8. Go to the Junos Space user interface > Job Management page to verify that the application is upgraded on the active site.

9. Upgrade the application on the standby site. To do so, type **/var/www/cgi-bin/./executeInstallAppOnDr.pl *application-image-name*** at the shell prompt of the active site and press Enter.

10. Verify the following on the standby site:
    - RPMs of the application are installed. To verify, execute the following command: **rpm -qa | grep <application-rpm-name>**.
    - **.ear** files of the application are available at **/usr/local/jboss/standalone/deployments/**.
11. Start the disaster recovery process on both sites from the active site. To do so, type **jmp-dr start** at the shell prompt of the VIP node at the active site and press Enter.

The Junos Space application is upgraded on the active and standby sites.

Uninstalling a Junos Space Application

You uninstall a Junos Space application from both sites to remove the application from your Junos Space deployment. You execute the **./executeUninstallAppOnDr.pl** script to uninstall an application.

To uninstall a Junos Space application from both sites:

1. Log in to the CLI of the Junos Space node at the active site on which the VIP or the eth0:0 interface is configured.

   The Junos Space Settings Menu is displayed.

2. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   You are prompted to enter the administrator password.

3. Enter the administrator password.

4. Stop the disaster recovery process on both sites. To do so, type **jmp-dr stop** at the shell prompt and press Enter.

5. Go to the Junos Space user interface > Administration workspace > Applications page to uninstall the application from the active site. Refer to "Uninstalling a Junos Space Application" on page 1406 in the *Junos Space Network Management Platform Workspaces Feature Guide*.

6. Go to the Junos Space user interface > Job Management page to verify that the application is completely removed from the active site.

7. Uninstall the application from the standby site. To do so, type **/var/www/cgi-bin/./executeUninstallAppOnDr.pl *ear-filename*** at the shell prompt at the standby site and press Enter.

   NOTE: You must add the filename without the extension (.ear) as follows:

   /var/www/cgi-bin/executeUninstallAppOnDr.pl aim

8. Verify the following on the standby site:
   - All database-related application data is removed.
   - RPMs of the application are removed. To verify, execute the following command: **rpm -qa | grep <application-rpm-name>**.
   - **.ear** files related to the application under **/usr/local/jboss/standalone/deployments/** are removed.
9. Start the disaster recovery process on both sites from the active site. To do so, type **jmp-dr start** at the shell prompt of the VIP node at the active site and press Enter.

The Junos Space application is uninstalled from the active and standby sites.

Adding or Removing a JBoss Node

We recommend that you meet the prerequisites to add a JBoss node or to know the impact of removing a JBoss node from the Junos Space setup. Refer to the "Adding a Node to an Existing Junos Space Fabric" on page 1176 and "Deleting a Node from the Junos Space Fabric" on page 1259 topics in the *Junos Space Network Management Platform Workspaces Feature Guide*. We also recommend that the active site and standby site be symmetric to ensure that the performance of the disaster recovery solution is effective and stable.

You add a JBoss node to improve the performance of your Junos Space setup. You remove a JBoss node if it is faulty and needs to be replaced. You may need to modify the disaster recovery configuration

depending on why you added or removed the JBoss node to or from the site. You execute the **./addNode.pl** or **./deleteNodeDR.pl** script to add or remove a JBoss node to or from the standby site.

To add or remove a JBoss node to or from both sites:

1. Log in to the CLI of the Junos Space node at the active site on which the VIP or the eth0:0 interface is configured.

   The Junos Space Settings Menu is displayed.

2. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   You are prompted to enter the administrator password.

3. Enter the administrator password.

4. Stop the disaster recovery process on both sites. To do so, type **jmp-dr stop** at the shell prompt and press Enter.

5. Go to the Junos Space user interface > Administration workspace > Fabric page to add or remove the JBoss node to or from the active site.

   - To add a JBoss node to the standby site, type **/var/www/cgi-bin/./addNode.pl SpaceNode <*name of the node*> <*node IP addess*> <*node user name*> <*node password*>** at the VIP node of the standby site and press **Enter**.

   - To delete a JBoss node from the standby site, type **/var/www/cgi-bin/./deleteNodeDR.pl <*node IP addess*>** at the VIP node of the standby site and press **Enter**.

6. Update the disaster recovery configuration on the active site. To do so, type **jmp-dr toolkit config update** at the shell prompt of the VIP node at the standby site and press Enter.

7. Update the disaster recovery configuration on the standby site. To do so, type **jmp-dr toolkit config update** at the shell prompt of the VIP node at the active site and press Enter.

8. (Optional) If you added a JBoss node with a different administrator password to a site, type **jmp-dr toolkit config update --user core** at the shell prompt of the VIP node at the peer site and press Enter.

9. Start the disaster recovery process on both sites from the active site. To do so, type **jmp-dr start** at the shell prompt at the active site and press Enter.

The JBoss node is added to or removed from the active and standby sites.

Adding or Removing a Dedicated Junos Space Node

We recommend that you meet the prerequisites to add a Junos Space node or to know the impact of removing a Junos Space node from a Junos Space setup. Refer to the "Adding a Node to an Existing Junos Space Fabric" on page 1176 and "Deleting a Node from the Junos Space Fabric" on page 1259 topics in the *Junos Space Network Management Platform Workspaces Feature Guide*. We also recommend that the active site and standby site be symmetric to ensure that the performance of the disaster recovery solution is efficient and stable.

You add a dedicated Junos Space node to improve the performance of your Junos Space setup. You remove a dedicated Junos Space node if it is faulty and needs to be replaced. You may need to modify the disaster recovery configuration depending on why you added or removed the dedicated Junos Space node to or from the site.

To add or remove a dedicated Junos Space node to or from both sites:

1. Log in to the CLI of the Junos Space node at the active site on which the VIP or the eth0:0 interface is configured.

   The Junos Space Settings Menu is displayed.

2. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   You are prompted to enter the administrator password.

3. Enter the administrator password.

4. Stop the disaster recovery process on both sites. To do so, type **jmp-dr stop** at the active site shell prompt and press Enter.

5. Go to the Junos Space user interface > Administration workspace > Fabric page to add or remove the dedicated Junos Space node to or from the active site. Refer to the "Adding a Node to an Existing Junos Space Fabric" on page 1176 and "Deleting a Node from the Junos Space Fabric" on page 1259 topics in the *Junos Space Network Management Platform Workspaces Feature Guide*.

6. Log in to the CLI of the Junos Space node at the standby site on which the VIP or the eth0:0 interface is configured.

   The Junos Space Settings Menu is displayed.

7. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   You are prompted to enter the administrator password.

8. Enter the administrator password.

9. Update the disaster recovery configuration on the standby site. To do so, type **jmp-dr toolkit config update** at the shell prompt of the VIP node at the standby site and press Enter.

10. Configure the current standby site as the active site. To do so, type **jmp-dr manualFailover** at the shell prompt and press Enter. For more information, see "Manually Failing Over the Network Management Services to the Standby Site" on page 1780.

11. Go to the Junos Space user interface > Administration workspace > Fabric page to add or remove the dedicated Junos Space node to or from the standby site.

12. Update the disaster recovery configuration on the active site. To do so, type **jmp-dr toolkit config update** at the shell prompt of the VIP node at the active site and press Enter.

13. Configure the original active site back as the active site. To do so, type **jmp-dr manualFailover** at the shell prompt and press Enter.

14. Start the disaster recovery process on both sites from the active site. To do so, type **jmp-dr start** at the shell prompt and press Enter.

The dedicated Junos Space node is added to or removed from the active and standby sites.

RELATED DOCUMENTATION

Disaster Recovery Overview | **1699**

Configuring the Disaster Recovery Process Between an Active and a Standby Site | **1731**

Viewing the Disaster Recovery Configuration and Status of Watchdog Services | **1752**

Modifying the Disaster Recovery Configuration | **1754**

Manually Failing Over the Network Management Services to the Standby Site

You may need to fail over the network management services to the standby site even when the active site is fully operational. You execute the **jmp-dr manualFailover** command at the standby site to fail over the network management services to the standby site. When the failover is complete, the standby site becomes the new active site.

> **NOTE:** We recommend that you check the status of the disaster recovery configuration before and after executing the **jmp-dr manualFailover** command. To do so, execute the **jmp-dr health** command at both sites.

To manually fail over the network management services to the standby site:

1. Log in to the CLI of the Junos Space node at the standby site on which the VIP or the eth0:0 interface is configured.

   The Junos Space Settings Menu is displayed.

2. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   The following is a sample output from a virtual appliance:

```
admin@10.206.41.183's password:
Last login: Mon Aug 17 06:17:58 2015 from 10.206.41.42

Welcome to the Junos Space network settings utility.

Initializing, please wait


Junos Space Settings Menu

1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> Expand VM Drive Size
7> (Debug) run shell
```

```
A> Apply changes
Q> Quit
R> Redraw Menu

Choice [1-7,AQR]: 7
```

You are prompted to enter the administrator password.

3. Enter the administrator password.

4. Type **jmp-dr manualFailover** at the shell prompt and press Enter.

5. Enter **Yes**.

   The following is a sample output:

```
[user1@host]# jmp-dr manualFailover
Do you really want to start manual failover: Yes
Check DR state of this site: started

INFO: => switchover DR at current site: active

Stop dr-watchdog if it's running
                        [ OK ]
Check status of DR remote site: up
Check current DR role: standby
Restore configuration files
                        [ OK ]
Setup MySQL replication: master-master
                        [ OK ]
Skip MySQL data backup
                        [ OK ]
Setup PostgreSQL replication
                        [ OK ]
Start file & RRD replication
                        [ OK ]
Open firewall for device traffic
                        [ OK ]
Start services(jboss,jboss-dc,etc.)
                        [ OK ]
Start dr-watchdog
                        [ OK ]
Copy files to DR slave site
```

```
                        [ OK ]
Update DR role of current site: active
                        [ OK ]

INFO: => switchover DR at DR remote site: standby

Check DR state of this site: started
Stop dr-watchdog if it's running
                        [ OK ]
Check status of DR remote site: up
Check current DR role: active
Stop services(jboss,jboss-dc,etc.)
                        [ OK ]
Block firewall for device traffic
                        [ OK ]
Reset MySQL init script and stop replication
                        [ OK ]
Skip MySQL data restore
                        [ OK ]
Setup MySQL replication and start replication
                        [ OK ]
Setup PostgreSQL replication
                        [ OK ]
Start files & RRD replication
                        [ OK ]
Start dr-watchdog
                        [ OK ]
Clean up /var/cache/jmp-geo/incoming
                        [ OK ]
Update DR role of current site: standby
                        [ OK ]
The manualFailover command is done.
The manualFailover command is done.
```

The standby site becomes the new active site.

NOTE:

If you have made any NAT-related updates in any of the disaster recovery sites, after a manual failover, run the following commands to ensure that NAT devices work seamlessly with the new active site:

1. Move the backup file from **/var/cache/jmp-geo/config/diff.properties_backup** to **/var/cache/jmp-geo/config/diff.properties**.
2. Run the following command on the VIP node to update the changed standby cluster device management, NAT, and IP configuration on the current active site:

   /var/cache/jmp-geo/script/toolkit-config-update.pl

RELATED DOCUMENTATION

- Disaster Recovery Overview | **1699**
- Configuring the Disaster Recovery Process Between an Active and a Standby Site | **1731**
- Stopping the Disaster Recovery Process | **1784**

Stopping the Disaster Recovery Process

You stop the disaster recovery process from the active site or the standby site when you need to update the disaster recovery configuration or add nodes or applications to the disaster recovery setup. You use the **jmp-dr stop** command to stop the disaster recovery process on both sites. Stopping the disaster recovery process does not clean up the disaster recovery configuration from the sites.

The **jmp-dr stop** command does the following:

- Stops the disaster recovery watchdog at the sites
- Stops the replication of MySQL data, PgSQL data, configuration files, and round-robin database (RRD) files between sites

We recommend that you execute the **jmp-dr health** command at both sites after you stop the disaster recovery process. This is to ensure that file replication, disaster recovery watchdog services, and other services are stopped. For more information, see "Checking the Status of the Disaster Recovery Configuration" on page 1747.

To stop the disaster recovery process at both sites:

1. Log in to the CLI of the Junos Space node at the active site on which the VIP or the eth0:0 interface is configured.

   The Junos Space Settings Menu is displayed.

2. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   The following is a sample output from a virtual appliance:

```
admin@10.206.41.183's password:
Last login: Mon Aug 17 06:17:58 2015 from 10.206.41.42

Welcome to the Junos Space network settings utility.

Initializing, please wait


Junos Space Settings Menu

1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
```

```
6> Expand VM Drive Size
7> (Debug) run shell

A> Apply changes
Q> Quit
R> Redraw Menu

Choice [1-7,AQR]: 7
```

You are prompted to enter the administrator password.

3. Enter the administrator password.

4. Type **jmp-dr stop** at the shell prompt and press Enter.

   The following is a sample output:

```
[user1@host]# jmp-dr stop
Check status of DR remote site: up
Check DR stop mode: both
Check current DR role: active
Stop order: DR remote site and then current

INFO: => stop DR at remote site

Check status of DR remote site: up
Check DR stop mode: solo
Check current DR role: standby
Stop dr-watchdog
                        [ OK ]
Stop mysql replication between sites
                        [ OK ]
Stop pgsql replication between sites
                        [ OK ]
Stop files & RRD replication
                        [ OK ]
The stop command is done.

INFO: => stop DR at current site: active

Stop dr-watchdog
                        [ OK ]
Stop files & RRD replication
```

```
                        [ OK ]
The stop command is done.
```

The disaster recovery process is stopped.

RELATED DOCUMENTATION

- Resetting the Disaster Recovery Configuration | 1786
- Modifying the Disaster Recovery Configuration | 1754
- Modifying Applications and Nodes on a Disaster Recovery Setup | 1765

Resetting the Disaster Recovery Configuration

You reset the disaster recovery configuration on both the active and the standby sites to stop the disaster recovery process and clean up the disaster recovery configuration from both sites. To reset the disaster recovery configuration, you execute the **jmp-dr reset** command.

The **jmp-dr reset** command does the following:

- Stops the disaster recovery watchdog at the sites
- Stops the replication of MySQL data, PgSQL data, configuration files, and round-robin database (RRD) files between sites
- Starts services such as JBoss, OpenNMS, Apache, and so on at the standby site
- Modifies the role of the cluster at the site (from active or standby to standalone)

To reset the disaster recovery configuration:

1. Log in to the CLI of the Junos Space node at the active site on which the VIP or the eth0:0 interface is configured.

   The Junos Space Settings Menu is displayed.

2. Enter **6** (if you are using a hardware appliance) or **7** (if you are using a virtual appliance) at the Junos Space Settings Menu prompt to run shell commands.

   The following is a sample output from a virtual appliance:

```
admin@10.206.41.183's password:
Last login: Mon Aug 17 06:17:58 2015 from 10.206.41.42

Welcome to the Junos Space network settings utility.

Initializing, please wait


Junos Space Settings Menu

1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> Expand VM Drive Size
7> (Debug) run shell

A> Apply changes
Q> Quit
R> Redraw Menu

Choice [1-7,AQR]: 7
```

You are prompted to enter the administrator password.

3. Enter the administrator password.

4. Type **jmp-dr reset** at the shell prompt and press Enter.

   The following is a sample output:

```
[user1@host]# jmp-dr reset
Check status of DR remote site: up
Check current DR role: active
Stop DR at both sites if it's running
                        [ OK ]
Clean up DR related tables in DB
                        [ OK ]
Clean up mysql repUser and repAdmin
                        [ OK ]
Clean up NTP
                        [ OK ]
```

```
Remove DR data
                          [ OK ]
Start services in standalone mode
                          [ OK ]
Remove DR configuration
                          [ OK ]
Clean up firewall
                          [ OK ]
Command completed.
```

5. To reset the disaster recovery configuration at the standby site, repeat steps 1 through 4 at the standby site.

The disaster recovery configuration is reset.

> **NOTE:** We recommend that you execute the **jmp-dr health** command on both sites after resetting the disaster recovery configuration to check the status of the role, disaster recovery process, services, replication process, and disaster recovery watchdog.

RELATED DOCUMENTATION

Configuring the Disaster Recovery Process Between an Active and a Standby Site | **1731**

Modifying the Disaster Recovery Configuration | **1754**

CHAPTER 100

Upgrading Junos Space Network Management Platform with Disaster Recovery Enabled

IN THIS CHAPTER

- Upgrade Procedure | 1789

Upgrade Procedure

IN THIS SECTION

- 1. Back up the Current Disaster Recovery Configuration | 1790
- 2. Reset the Disaster Recovery Configuration | 1790
- 3. Upgrade the Junos Space Network Management Platform and Application | 1790
- 4. Configure and Perform Disaster Recovery | 1793

You must reset the disaster recovery configuration on both the active and the standby sites to stop the disaster recovery process and clean up the disaster recovery configuration from both the sites. You can upgrade the Junos Space Platform software at both the active and the standby sites at the time of deployment. Since the disaster recovery upgrade procedure is time consuming, we recommend you to reset the disaster recovery configuration and upgrade the sites to the required version.

The upgrade procedure comprises of the following tasks:

1. Back up the Current Disaster Recovery Configuration
2. Reset the Disaster Recovery Configuration

3. Upgrade the Junos Space Network Management Platform and Application
4. Configure and Perform Disaster Recovery

1. Back up the Current Disaster Recovery Configuration

Backup the current disaster recovery configuration on both the sites to refer the parameters when configuring the disaster recovery again after upgrade. Run the following command to create a backup for current configuration on both sites:

$ jmp-dr api v1 config --include role,failover,states,core,deviceManagement,mysql,pgsql,file,watchdog > /home/admin/dr-config.txt

> **NOTE:** Enter the following command in a separate shell prompt on the VIP nodes of both the sites to check log errors:
> **$tailf /var/log/jmp-geo/dr-cli-reset.log**

2. Reset the Disaster Recovery Configuration

Reset the current disaster recovery configuration to ensure that both the active and the passive sites refer to the same parameters, when you configure the disaster recovery, post the upgrade.

Execute the following command to create a backup for the current configuration.

$ jmp-dr api v1 config --include role,failover,states,core,deviceManagement,mysql,pgsql,file,watchdog > /home/admin/dr-config.txt

Execute the following commands to reset disaster recovery on both sites running the **jmp-dr reset** commands on VIP nodes of both sites.

```
$jmp-dr reset
```

After executing this commands, the sites become standalone sites. Junos Space Platform comes up and you can access the UI from both the sites.

3. Upgrade the Junos Space Network Management Platform and Application

You can upgrade the Junos Space Platform and the application on both the active and the standby sites simultaneously, as both the sites are in standalone mode.

To upgrade the Junos Space Network Management Platform:

1. Login to the Junos Space Network Management Platform.

   The dashboard appears.

2. Upload the software image to the active and standby sites.

   a. Select **Network Management Platform** from the **Applications** drop-down menu.

   b. Click **Upgrade**.

      The upgrade window appears.

   c. Upload the image.

      NOTE: The system takes approximately 5 minutes to upload the new image. Enter the following command in a separate shell prompt at each node of current active and standby sites to check the logs for errors.

      $tailf /var/log/install.log

3. Upgrade the Junos Space software at the active and standby sites.

   Reboot occurs as part of post upgrade.

   a. Select **Network Management Platform > Administration > Application > Network Management Platform**.

   b. Click **Upgrade**.

      The upgrade window appears.

   c. In the **Upload Platform** menu, select the specific row and click **Upgrade**.

      The maintenance mode screen displays the upgrade progress. The reboot screen appears, once the upgrade is completed.

      NOTE: Type the following command in the separate shell prompt on each node of current active and standby sites to check the error logs.

      $tailf /var/log/install.log .

> **NOTE:** Type the following command in a separate shell prompt at each node on the active and standby sites to check the upgrade progress.
>
> **$tailf /var/jmp_upgrade/slave/log/<oldRelease_newRelease>**

d. Click **Reboot**.

The nodes starts to reboot.

> **NOTE:** Execute the following command to check for boot to complete.
>
> **$tail -f /tmp/systemStartup.log**
>
> Log Example:
> **2018/03/07 10:05:51.207 Appmgt is now deploying ... [9 of 9] 2018/03/07 10:05:57.607 Appmgt**

4. Upload the Junos Space application in active and the standby site.

a. Select **Network Management Platform > Administration > Application >*<application-name>*> Upgrade > Action**.

b. Click **Upload**.

The upload window appears.

c. Upload the selected Junos Space application.

> **NOTE:** Enter the following command in the separate shell prompt on each node of current active and standby sites to check the logs for errors.
>
> **$tailf /var/log/install.log**

5. Upgrade the Junos Space application in the active and standby site.

a. Select **Network Management Platform > Administration > Application >*<application-name>*> Upgrade > Action**.

b. Click **Upgrade**.

The Upgrade window appears.

c. In the **Upgrade Application** menu, select the specific row and click **Upgrade**.

> **NOTE:** Enter the following command in a separate shell prompt on each node of current active and standby sites to check the logs for error.
>
> **$tailf /var/log/install.log**

d. Select **Network Management Platform > Administration > Application**.

The Application window displays the expected upgrade version.

4. Configure and Perform Disaster Recovery

> **NOTE:** This is an optional procedure. If you plan to configure multiple upgrade paths: upgrade the Junos Space Network Management Platform and the application to the required version, before you configure disaster recovery.

To configure and start the disaster recovery process on both the active and the passive sites:

1. Configure the disaster recovery process.
   a. Execute the following command in the VIP node of active site to configure disaster recovery.

```
$ jmp-dr init –a
```

   b. Execute the following command in the VIP node of standby site to configure disaster recovery.

```
$ jmp-dr init –s
```

> **NOTE:** Ensure that you initialize the disaster recovery process on the standby site, only after the disaster recovery initialization is complete on the active site. For more information about configuring the disaster recovery process, see Configuring the Disaster Recovery Process Between an Active and a Standby Site.

2. Execute the following command to start the disaster recovery process from the active site.

```
jmp-dr start
```

> **NOTE:** Execute the following command in the separate shell prompt on each of the VIP nodes of the site to check the logs for errors.
>
> ```
> $tailf /var/log/jmp-geo/dr-cli-start.log
> ```

If the standby node is not updated, stop and the start the disaster recovery process over again.

Execute the command again for verify the update.

3. Execute the following command to check the disaster recovery process health:

```
$jmp-dr health
```

> **NOTE:** Execute the following command in a separate shell prompt on each site VIP nodes to check the logs for errors:
>
> ```
> $tailf /var/log/jmp-geo/dr-cli-health.log
> ```

4. Execute the following command to stop the disaster recovery process on both the sites from the active site:

```
$jmp-dr stop
```

NOTE: Execute the following command in the separate shell prompt on each VIP nodes of the site to check the logs for errors:

```
$tailf /var/log/jmp-geo/dr-cli-stop.log
```

5. Execute the following command on the current standby site, to verify the functionality on standby site by manually fail-over from active site:

```
$jmp-dr manualFailover
```

NOTE: Execute the following command in the separate shell prompt on VIP node of the standby site to check the logs for error:

```
$tailf /var/log/jmp-geo/dr-cli-manual-failover.log
```

NOTE: Execute the following command to verify is the application starts normally, by checking the JBoss log:

```
$tailf /var/log/jboss/server/server1/server.log
```

The Application page shows the upgrade version.

6. Execute the following command on the current standby site VIP node to apply manual fail-over to the active site from the standby site:

```
$jmp-dr manualFailover
```

NOTE: Execute the following command in the separate shell prompt on VIP node of the current standby site to check the logs for errors.

```
$tailf /var/log/jmp-geo/dr-cli-manual-failover.log
```

NOTE: Execute the following command to check for the application start by checking the JBoss log:

```
$tailf /var/log/jboss/server/server1/server.log
```

7. Execute the following command to check the disaster recovery health on both the sites.

```
$jmp-dr health
```

NOTE: Execute the following command in the separate shell prompt on each VIP nodes of the site to check the logs for errors.

```
$tailf /var/log/jmp-geo/dr-cli-health.log
```

8. Execute the following command to start the disaster recovery process on both the sites from active site.

```
$jmp-dr start
```

NOTE: Execute the following command in the separate shell prompt on each VIP nodes of the site to check the logs for errors.

```
$tailf /var/log/jmp-geo/dr-cli-start.log
```

9. Execute the following command to check the disaster recovery process health on both sites.

```
$jmp-dr health
```

NOTE: Execute the following command in the separate shell prompt on each VIP nodes of the site to check the logs for errors.

```
$tailf /var/log/jmp-geo/dr-cli-health.log
```

RELATED DOCUMENTATION

Configuring the Disaster Recovery Process Between an Active and a Standby Site | 1731

Modifying the Disaster Recovery Configuration | 1754