

Junos Space Network Management Platform Release 15.1R4 Release Notes

Release 15.1R4
11 Oct 2017

Contents

Junos Space Network Management Platform Release Notes	3
Installation Instructions	3
Upgrade Instructions	4
Instructions for Validating the Junos Space Network Management Platform OVA Image	4
Upgrading from Prior Releases of Junos Space Network Management Platform	4
Reboot Sequence After Upgrading on a Multinode Setup	4
Upgrade Notes	5
Application Compatibility	6
Supported Junos Space Applications and Adapters	6
Supported Hardware	7
Supported Devices	7
New and Changed Features	8
New and Changed Features in Junos Space Network Management Platform Release 15.1R4	9
New and Changed Features in Junos Space Network Management Platform Release 15.1R3	9
New and Changed Features in Junos Space Network Management Platform Release 15.1R2	9
New and Changed Features in Junos Space Network Management Platform Release 15.1R1	9
Operational Notes	14
Changes in Default Behavior	18
Known Behavior	18
Known Issues	23
Resolved Issues	33
Documentation Updates	34
Junos OS Compatibility	34
Junos Space Documentation and Release Notes	34

Requesting Technical Support	35
Self-Help Online Tools and Resources	35
Opening a Case with JTAC	35
Revision History	37

Junos Space Network Management Platform Release Notes

These release notes accompany Junos Space Network Management Platform Release 15.1R4

- [Installation Instructions on page 3](#)
- [Upgrade Instructions on page 4](#)
- [Application Compatibility on page 6](#)
- [Supported Junos Space Applications and Adapters on page 6](#)
- [Supported Hardware on page 7](#)
- [Supported Devices on page 7](#)
- [New and Changed Features on page 8](#)
- [Operational Notes on page 14](#)
- [Changes in Default Behavior on page 18](#)
- [Known Behavior on page 18](#)
- [Known Issues on page 23](#)
- [Resolved Issues on page 33](#)
- [Documentation Updates on page 34](#)
- [Junos OS Compatibility on page 34](#)

Installation Instructions

Junos Space Network Management Platform Release 15.1R4 can be installed on a Junos Space Appliance or a Junos Space Virtual Appliance.



CAUTION: During the Junos Space Network Management Platform installation process, 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 fails.

- For installation instructions for a JA1500 Junos Space Appliance, refer to the [Installation and Configuration](#) section of the [JA1500 Junos Space Appliance Hardware Guide](#).
- For installation instructions for a JA2500 Junos Space Appliance, refer to the [Installation and Configuration](#) section of the [JA2500 Junos Space Appliance Hardware Guide](#).
- For installation instructions for a Junos Space Virtual Appliance, refer to the [Deploying the Junos Space Virtual Appliance](#) section of the [Junos Space Virtual Appliance Installation and Configuration Guide](#).

Refer to the “[Supported Hardware](#)” on [page 7](#) for more information about the hardware supported.

Upgrade Instructions

This section includes instructions to upgrade to Junos Space Network Management Platform Release 15.1R4. Read these instructions before you begin the upgrade process.



CAUTION: During the Junos Space Network Management Platform upgrade process, 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.

- [Instructions for Validating the Junos Space Network Management Platform OVA Image](#)
- [Upgrading from Prior Releases of Junos Space Network Management Platform](#)
- [Reboot Sequence After Upgrading on a Multinode Setup](#)
- [Upgrade Notes](#)

[Instructions for Validating the Junos Space Network Management Platform OVA Image](#)



NOTE: In Junos Space Platform Release 15.1R4, the validation of the Junos Space Platform open virtual appliance (OVA) image using the Juniper Networks Root CA certificate chain file is not supported because the certificate chain file is not available for Release 15.1R4.

[Upgrading from Prior Releases of Junos Space Network Management Platform](#)

You can upgrade to Junos Space Network Management Platform Release 15.1R4 from the following prior releases:

- 15.1R1
- 15.1R2
- 15.1R3



NOTE: You can also upgrade from Junos Space Platform Releases 14.1R1, 14.1R2, and 14.1R3 by first upgrading to Release 15.1R1 and then to Release 15.1R4.

[Reboot Sequence After Upgrading on a Multinode Setup](#)

When you upgrade to Junos Space Network Management Platform Release 15.1R4 on a multinode setup, you must initiate a reboot after the upgrade is complete. Junos Space Platform reboots all nodes simultaneously.

Upgrade Notes

- During the upgrade process, do not manually reboot the nodes if the Junos Space user interface does not come up for an extended period of time. Contact the Juniper Networks Support team for help in resolving this issue.
- Before the upgrade, ensure that the latest backups are available in a location other than the Junos Space server. For more information about backups, see *Backing Up the Junos Space Network Management Platform Database* (in the *Workspaces Feature Guide*).
- Before starting the upgrade process, ensure that none of the nodes on the Junos Space fabric contains a large number of database backups in the `/var/cache/jboss/backup` directory. Large number of database backups may delay the initialization process. We recommend that you retain only the previous two database backups before starting the upgrade process. Delete all other database backups before starting the upgrade process.
- After the upgrade process is complete, check the status of all nodes in the Junos Space fabric (in the **Administration** > **Fabric** page) and ensure that the **Status** is **UP** for all nodes *before* you start upgrading a Junos Space application. Otherwise, the software upgrade may fail across all nodes.
- When you upgrade to Junos Space Platform Release 15.1R4, if there is a failure in one of the steps in the upgrade process, the subsequent steps are not executed. After the upgrade is completed, the **Upgrade Status Summary** field (in the Software Install Status dialog box) displays warning messages, information about the error that led to the upgrade failure, and the location of the log files for troubleshooting.
- If you are upgrading a Junos Space fabric (running Junos Space Platform releases 14.1R1 or 14.1R2) that contains Fault Monitoring and Performance Monitoring (FMPM) node to Junos Space Network Management Platform Release 15.1R4, add the entry `\var\www\specialNodeAgent-bin\secure\swInstallSpecialNode.pl` to the `/usr/nma/lib/nmaSecurityScriptsWhitelist.rules` file in all the nodes *before* the upgrade, and then perform the upgrade.
- If you are managing devices running ScreenOS (as unmanaged devices) on a prior release of Junos Space Platform and upgrade to Junos Space Platform Release 15.1R4, you can no longer manage devices running ScreenOS as unmanaged devices after the upgrade. In addition, you cannot model ScreenOS devices using the Model Devices feature.
- If the administrator password for an FMPM node is modified because of password expiry or by using the Junos Space CLI, *before* uploading the Junos Space Platform image, ensure that you run the `/var/www/cgi-bin/changeSpecialNodepassword.pl` script on the Junos Space VIP node so that the modified FMPM node password is updated in the Junos Space MySQL database.

To update the modified FMPM node password:

1. Connect to the Junos Space VIP node (by using SSH) and log in (as the **admin** user) to access the Junos Space CLI.

The Junos Space Settings Menu appears.

2. Type **6** (if the node is a hardware appliance) or **7** (if the node is a virtual appliance) to open a debug (command) prompt.

You are prompted to enter your password.

3. Type the password for the **admin** user and press Enter.

You are taken to the shell.

4. Change the directory to `/var/www/cgi-bin/` by executing the following command:
`cd /var/www/cgi-bin/`.

5. Run the `/var/www/cgi-bin/changeSpecialNodePassword.pl` script as follows:

```
/var/www/cgi-bin/changeSpecialNodePassword.pl fmpm-node-ip  
fmpm-node-password
```

where *fmpm-node-ip* is the IP address of the FMPM node, and *fmpm-node-password* is the modified password for the FMPM node.

If the password change is successful, a confirmation message that the password is changed is displayed.

6. Log out of the Junos Space VIP node.

Application Compatibility



WARNING: Before you upgrade to Junos Space Network Management Platform Release 15.1R4, ensure that compatible versions of Junos Space applications are available for upgrade by referring to the [Junos Space Application Compatibility](#) knowledge base article. If you upgrade to Junos Space Network Management Platform Release 15.1R4 and the compatible version of a Junos Space application is not available, the current version of the Junos Space application is deactivated and cannot be used until Juniper Networks releases a compatible version of the Junos Space application.

Supported Junos Space Applications and Adapters

This release of Junos Space Network Management Platform supports the following Junos Space applications:

- Connectivity Services Director Release 1.0R1
- Cross Provisioning Platform 15.1R1
- Edge Services Director 1.0R1
- Network Director Release 2.5R1
- Security Director Release 15.1R2
- Service Now releases 14.1R1, 14.1R2, 14.1R3, 14.1R4, 15.1R2, 15.1R3, 15.1R4, and 16.1R1



NOTE: Service Now releases 14.1R1, 14.1R2, 14.1R3, 14.1R4, and 15.1R2 are supported only when you upgrade to Junos Space Platform Release 15.1R4 and not on a clean installation of Junos Space Platform Release 15.1R4.

- Service Insight releases 14.1R1, 14.1R2, 14.1R3, 14.1R4, 15.1R2, 15.1R3, 15.1R4, and 16.1R1



NOTE: Service Insight releases 14.1R1, 14.1R2, 14.1R3, 14.1R4, and 15.1R2 are supported only when you upgrade to Junos Space Platform Release 15.1R4 and not on a clean installation of Junos Space Platform Release 15.1R4.

- ww Junos OS Adapter

For the latest information, see the [Junos Space Application Compatibility](#) knowledge base article.

Supported Hardware

Junos Space Network Management Platform Release 15.1R4 can be installed on the following hardware:

- JA1500 Junos Space Appliance
- JA2500 Junos Space Appliance
- VMware ESX server 4.0 or later or VMware ESXi server 4.0, 5.0, 5.1, or 5.5
- Kernel-based virtual machine (KVM) (Release 0.12.1.2-2/448.el6 or later) server installed on CentOS Release 6.5

For detailed information about hardware requirements, refer to the *Hardware Documentation* section of the *Junos Space and Applications* page.

Supported Devices

No additional Juniper Networks devices are supported in Junos Space Network Management Platform Release 15.1R4.

For a complete list of supported devices supported up to Junos Space Platform Release 15.1R1, see *Which Juniper Networks Devices Does Junos Space Network Management Platform Support?* in the [Junos Space Device Management FAQ](#) topic. For a list of devices supported in Junos Space Platform Release 15.1R2, see the [Junos Space Network](#)

[Management Platform Release 15.1R2 Release Notes](#). For a list of devices supported in Junos Space Platform Release 15.1R3, see the [Junos Space Network Management Platform Release 15.1R3 Release Notes](#).



NOTE: When Junos Space Platform discovers EX Series switches running Layer 2 next-generation (L2NG) software, the device family for these devices is displayed (on the Device Management page) as junos and not as junos-ex. This behavior is currently observed on EX4300 and EX9200 switches running Layer 2 next-generation software.

New and Changed Features

- [New and Changed Features in Junos Space Network Management Platform Release 15.1R4](#)
- [New and Changed Features in Junos Space Network Management Platform Release 15.1R3](#)
- [New and Changed Features in Junos Space Network Management Platform Release 15.1R2](#)
- [New and Changed Features in Junos Space Network Management Platform Release 15.1R1](#)

New and Changed Features in Junos Space Network Management Platform Release 15.1R4

- No new features are introduced in Junos Space Network Management Platform Release 15.1R4.

New and Changed Features in Junos Space Network Management Platform Release 15.1R3

- No new features are introduced in Junos Space Network Management Platform Release 15.1R3.

New and Changed Features in Junos Space Network Management Platform Release 15.1R2

- No new features are introduced in Junos Space Network Management Platform Release 15.1R2.

New and Changed Features in Junos Space Network Management Platform Release 15.1R1

This section describes new features and the enhancements to existing features in Junos Space Network Management Platform Release 15.1R1.

- **IPv6 support for nodes in the Junos Space fabric**—From Junos Space Network Management Platform Release 15.1R1 onward, you can configure nodes in the Junos Space fabric with only IPv4 addresses or both IPv4 and IPv6 addresses (dual stack). For more information, see *Junos Space IPv6 Support Overview* (in the *Workspaces Feature Guide*).
- **Validation of SSH fingerprints**—You can validate the SSH fingerprints of up to 1024 devices simultaneously by using the Device Discovery workflow. Junos Space Platform stores the SSH fingerprints in the database and validates them during subsequent connections with the device. If you do not specify an SSH fingerprint during the Device Discovery workflow, Junos Space Platform obtains SSH fingerprint details from the device when it connects to Junos Space Platform for the first time. 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 UI or automatically by Junos Space Platform:

- To manually resolve a fingerprint conflict, initiate the Acknowledge Device Fingerprint workflow from the Devices workspace.
- To allow Junos Space Platform to automatically update SSH fingerprints, disable the **Manually Resolve Fingerprint Conflict** check box on the Modify Application Settings page (**Administration > Applications > Network Management Platform > Modify Application Setting**).

Junos Space Platform checks whether the SSH fingerprints on a device and in the Junos Space Platform database match when staging scripts on the device, executing scripts on the device, staging a device image on the device, deploying a device image on the device, connecting to the device by using SSH, and reactivating a replacement device.

For more information, see *Device Authentication in Junos Space* and *Modifying Junos Space Network Management Platform Settings* (in the *Workspaces Feature Guide*).

- **Organization of scripts based on category**— From Junos Space Network Management Platform Release 15.1R1 onward, you can organize scripts based on the category of the scripts. You can add the @CATEGORY annotation to script contents and filter scripts based on the value you set. The category field for scripts is displayed on pages or in dialog boxes in the following workspaces:

- Images and Scripts workspace:
 - Scripts Inventory
 - View Associated Devices
 - View Execution Results
 - Create/Edit Operation (Select Scripts)
 - Create Script Bundle
 - Modify Script Bundle
- Jobs workspace:
 - Script Management Job Status
 - Script Execution Job Result
- Devices workspace:
 - View Associated Scripts
 - View Script Executions
 - Execute Scripts

For more information, see *Scripts Overview* (in the *Workspaces Feature Guide*).

- **Enhancements to the disaster recovery solution for warm standby**—The Junos Space Platform disaster recovery solution includes the following enhancements:
 - Disaster recovery between the active and the standby sites from the VIP nodes at the sites by using CLI commands
 - Automatic failover from the active to the standby sites based on the built-in device—arbitration algorithm or custom failure scripts within 20 to 30 minutes of a disaster
 - Asynchronous replication of MySQL and PostgreSQL databases from the active to the standby sites over an encrypted connection
 - Display of the overall status of the disaster recovery configuration and the status of disaster recovery watchdog services at a site by using CLI commands

- Manual failover to the standby site by using a single CLI command when the active site needs to be shut down for maintenance activities
- Modification of a specific part of the disaster recovery configuration at a site, or resetting or stopping of the disaster recovery process at both sites by using CLI commands. Resetting the disaster recovery configuration erases the disaster recovery configuration from both sites and converts them to standalone clusters.

For more information, see *Disaster Recovery Overview* (in the *High Availability and Disaster Recovery Guide*).

- **Export and import of Configuration Views**—From the CLI Configlets workspace, you can export and import Configuration Views in XML format. Junos Space Platform performs an integrity check on the Configuration Views that you are about to import, reports any errors, and allows you to either overwrite or cancel the importing process. You can export all Configuration Views from the Junos Space Platform database except the Default View. For more information, see *Configuration Views Overview* (in the *Workspaces Feature Guide*).
- **Upgrade checks**—From Junos Space Platform Release 15.1R1 onward, the system checks whether the following requirements are met before you can upgrade the software:
 - Free disk space—If a node or cluster fails to meet the minimum disk requirement of 10 GB in the root partition, an error message is displayed indicating the IP address of the node or cluster. If you receive this error message, you cannot continue the upgrade process.
 - Active MySQL replication and PostgreSQL replication processes—If the MySQL replication or PostgreSQL replication processes are turned off on any of the nodes, a warning message is displayed. If you receive this warning message, you can either continue or stop the upgrade process.

If both the preceding requirements are not met, an error message is displayed and the upgrade process is not initiated.

- **Enhancements to rebooting of fabric nodes**—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.
- **Enhancements to error reporting during the upgrade process**—When you upgrade to Junos Space Platform Release 15.1R1, if there is a failure in one of the steps in the upgrade process, the subsequent steps are not executed. After the upgrade is completed, the **Upgrade Status Summary** field (in the Software Install Status dialog box) displays warning messages, information about the error that led to the upgrade failure, and the location of the log files for troubleshooting.
- **Enhancements to improve the overall stability**—In Junos Space Network Management Platform Release 15.1R1, several enhancements have been made to the upgrade, failover, and related processes that improve the overall stability of Junos Space Platform.

- **Ability to run the MySQL database on dedicated database nodes**—From Junos Space Network Management Platform Release 15.1R1 onward, you can add dedicated database nodes to the Junos Space fabric and run the MySQL database server on those nodes.

You can add two nodes as the primary and secondary database nodes, providing database high availability. The MySQL database is moved to the database nodes and disabled on the Junos Space active and standby nodes, improving the performance of the Junos Space active node. The MySQL database servers on the database nodes are accessed using a database VIP address that is different from the Junos Space fabric VIP address.

After you add dedicated database nodes, the database cannot be moved back to the Junos Space active and standby nodes. You can delete either the primary or secondary database node, but not both nodes.

For more information, see *Fabric Management Overview* (in the *Workspaces Feature Guide*).

- **Purging policy and framework for purging backup files and logs**—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.

For more information, see *Junos Space Purging Policy and Purging Categories Overview* (in the *Workspaces Feature Guide*).

- **Junos Space debug utilities**—You can execute the scripts and Java applications located at `/var/log/space-debug/debug-utilities` of a Junos Space node to fetch details that you cannot view on the JBoss CLI or the Junos Space UI. These scripts and Java applications are categorized under the **deviceConnection**, **jobManagement**, **deviceImport**, and **HornetQ** directories:
 - You can view details and troubleshoot device connection, device resynchronization, and node connection issues by executing the device connection and device import debug utilities.
 - You can view information about the jobs executed on a Junos Space node and the resources allocated for these jobs and processes, such as JBoss, Apache Web Proxy, MySQL, Network Monitoring, and PostgreSQL, on all Junos Space nodes by executing the job management debug utilities.
 - You can view details about all JBoss queues or view the list of messages on a specific queue by executing the HornetQ debug utilities.

You can view the output from these scripts and Java applications on the CLI of the node or from the text output files stored on the node. The scripts and Java applications are as follows:

- Device connection debug scripts—**getDeviceInfo.sh**, **DeviceDebugInfoCollector.sh**, **getAllDeviceInfo.sh**, and **cleanupEditChannel.sh**
- Device import scripts and Java applications—**cleanupDeviceImportTables.sh** and **DB-blob-reader.jar**

- Job management scripts and Java applications—**SystemLoadViewer.sh**, **getJobThreadSump.sh**, and **JobInfoCollector.jar**
- HornetQ scripts—**HornetQInfoProvider.sh** and **HQMessageViewer.sh**
- **Option to determine whether Network Monitoring monitors only Junos Space fabric nodes or both devices and fabric nodes**—The **Disable network monitoring for all devices** check box on the Modify Application Settings page determines whether Network Monitoring is used to monitor only Junos Space fabric nodes (check box is cleared, which is the default) or both Junos Space fabric nodes and devices (check box is selected). For more information, see *Modifying Junos Space Network Management Platform Settings* (in the *Workspaces Feature Guide*).
- **Enhancement to resynchronization of nodes in Network Monitoring**—The Resync Nodes job has been enhanced to support subjobs that are distributed across the available Junos Space nodes.
- **Enhancements to REST APIs**—From Junos Space Network Management Platform Release 15.1R1 onward, the login and logout Representational State Transfer (REST) methods are added to enable RESTful API single sign-on (SSO) sessions and define the session scope. Any REST APIs executed outside the session scope do not participate in the RESTful session. REST APIs executed within the range of this scope are authenticated and do not require the use of credentials or X.509 certificates.
- **Installation and management of Junos Continuity software packages**—You can install and manage Junos Continuity software packages from the Images and Scripts workspace of Junos Space Platform. Junos Space Platform allows you to manage Junos Continuity software packages on the MX240, MX480, MX960, MX2010, and MX2020 platforms. You can perform all the tasks that can be performed on device image files, apart from modifying the device series, on Junos Continuity software packages. In addition, you can undeploy Junos Continuity software packages from devices. For more information, see *Device Images Overview* (in the *Workspaces Feature Guide*).
- **Access control checks for report definitions and reports**—Access control checks ensure the following:
 - Reports generated from the parent domain contain information from all subdomains.
 - Reports generated from a subdomain contain information only from that subdomain.
 - Reports contain information from all accessible domains only if you set the **Manage objects from all assigned domains** flag. To set this flag, click the **User Settings** icon on the Junos Space banner.
 - You can perform jobs such as creating, modifying, cloning, or deleting report definitions and generating, viewing, or deleting reports only if you have access to the specific report type in the report definition or report.

For more information, see *Reports Overview* (in the *Workspaces Feature Guide*).

- **Support for canceling multiple jobs**—From Junos Space Network Management Platform Release 15.1R1 onward, you can select and cancel multiple jobs from the Jobs workspace simultaneously. For more information, see *Canceling Jobs* (in the *Workspaces Feature Guide*).

- **Scheduling of the download of troubleshooting log files**—You can schedule when to download troubleshooting log files from the Junos Space Platform database through the Job Management page. For more information, see *Downloading the Troubleshooting Log File in Server Mode* (in the *Workspaces Feature Guide*).
- **Support for archiving and purging jobs of a particular job type**—From Junos Space Network Management Platform Release 15.1R1 onward, you can select jobs of a particular job type for archiving and purging. For more information, see *Archiving and Purging Jobs* (in the *Workspaces Feature Guide*).
- **Selection of devices by domain during configuration files backup**—From Junos Space Network Management Platform Release 15.1R1 onward, while backing up configuration files you can select devices based on the domain to which the devices belong. For more information, see *Backing Up Configuration Files* (in the *Workspaces Feature Guide*).
- **Vendor part number and vendor material number information in the physical inventory**—From Junos Space Network Management Platform Release 15.1R1 onward, you can view the vendor part number and vendor material number associated with a device on the View Physical Inventory page. In addition, when you export the physical inventory details, the **Vendor Part Number** and **Vendor Material Number** columns are exported along with other information. For more information, see *Device Inventory Overview* (in the *Workspaces Feature Guide*).
- **Option to purge or archive and purge audit logs from all domains to which you have access**—From Junos Space Network Management Platform Release 15.1R1 onward, you can purge or archive and purge audit logs from all domains to which you have access by selecting the **Purge audit logs from all accessible domains** check box (**Audit Logs > Audit Log > Archive/Purge Logs**). For more information, see *Archiving and Purging or Only Purging Audit Logs* (in the *Workspaces Feature Guide*).

Operational Notes

The following are the operational notes for Junos Space Network Management Platform Release 15.1R4:

- If you select the **Add SNMP configuration to device** check box on the **Administration > Applications > Modify Network Management Platform Settings** page and discover a device whose trap target is updated, clicking Resync Node from the Network Monitoring workspace does not reset the trap target for the device.
- If you clear the **Add SNMP configuration to device** check box on the **Administration > Applications > Modify Network Management Platform Settings** page, the trap target is not set for the device during device discovery and resynchronizing node operations.
- If you want to perform a global search by using partial keywords, append "*" to the search keywords.
- To perform a partial keyword search on tags on the Tags page (**Administration > Tags**) or the Apply Tags dialog box (right-click a device in the **Device Management** page and select **Tag It**), append * to the search keyword.
- Job Administrator privileges are required to cancel auto generated Resync Network Elements jobs.

- Internet Explorer slows down because some scripts may take an excessive amount of time to run. The browser prompts you to decide whether to continue running the slow script. Refer to <http://support.microsoft.com/kb/175500> for instructions on to fix this issue.
- When you switch from "Space as system of record" mode to "Network as system of record" mode, devices with the "Managed Status: 'Device Changed' or 'Space & Device Changed'" status are automatically synchronized after 900 seconds. To reduce this time period, modify the **Polling time period secs** setting for Network Management Platform (**Administration > Applications > Modify Application Settings**) to a lower value such as 150 seconds.
- In Space as System of Record (SSoR) mode on Junos Space, when a new authentication key is generated, devices discovered and managed using RSA keys whose management status is Device Changed move to the Key Conflict Authentication status. To resolve the conflict on the devices and bring them back to a key-based state, upload the RSA keys manually (**Devices > Upload Keys to Devices**).
- Devices such as the BX Series and MCG5000 devices that do not use system status log files are not supported in Space as System of Record (SSoR) mode.
- The **EnterpriseDefault** (uei.opennms.org/generic/trap/EnterpriseDefault) event appears on the Events page in the Network Monitoring workspace only if there is no associated event definition for a received event. To create the required event definition, compile the MIB corresponding to the object ID (OID). You can find the OID by reviewing the details of the **EnterpriseDefault** event.

For more information about compiling SNMP MIBs, refer to the [Compiling SNMP MIBs](#) topic.

- When a physical hard drive is removed from a Junos Space hardware appliance (JA1500 or JA2500) or a logical hard drive is degraded, the corresponding SNMP traps (`jnxSpaceHardDiskPhysicalDriveRemoved` and `jnxSpaceHardDiskLogicalDeviceDegraded` respectively) are generated and displayed as events in the Network Monitoring workspace. Later, when the physical hard drive is reinserted, the corresponding events (`jnxSpaceHardDiskPhysicalDriveAdded` and `jnxSpaceHardDiskLogicalDeviceRebuilding`) are generated and displayed in the Network Monitoring workspace; however, the alarms previously raised for the removal of the physical hard drive are not cleared automatically. You can clear these alarms manually, if required. The alarms for the reinsertion of the physical hard drive are automatically cleared after a few minutes because they are of the **Normal** type.
- If the administrator password for a Fault Monitoring and Performance Monitoring (FMPM) node is modified using the Junos Space CLI, the disaster recovery with the FMPM node fails and new users added in Junos Space (after the password is modified) are not synchronized to the FMPM node. This is because the modified administrator password is not automatically updated in the Junos Space MySQL database.

To ensure that the synchronization to the FMPM node takes place, you must run the `/var/www/cgi-bin/changeSpecialNodepassword.pl` script so that the modified FMPM node password is updated in the Junos Space MySQL database. The syntax for the script is as follows: `/var/www/cgi-bin/changeSpecialNodePassword.pl fmpm-node-ip`

fmpm-node-password, where *fmpm-node-ip* is the IP address of the FMPM node, and *fmpm-node-password* is the modified password for the FMPM node.

- Junos Space Network Management Platform Release 15.1R4 uses OpenSSL version openssl-0.9.8e-33.el5_11. Although this version is based on the older 0.9.8e branch, it contains all relevant security updates and fixes (current up to the April 2015 release) provided by OpenSSL and CentOS. For further details regarding fixes and CVEs included in this OpenSSL version, execute the following command on the Junos Space debug shell: **rpm -q openssl-0.9.8e-33.el5_11 -changelog**.

- 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.

- Junos Space Network Management Platform Release 15.1R4 does not fully support the management of devices behind Network Address Translation (NAT). However, you can use Junos Space Platform to manage devices behind NAT (only for device-initiated connections) by using the Model/Activate Devices workflow, excluding some actions listed below, which require the IP address of the device:
 - You cannot use the network monitoring functionality.
 - You cannot use the device Web GUI.
 - You cannot use key-based authentication.
 - You cannot connect to a device by using SSH.
 - You cannot activate a device that is in the Return Materials Authorization (RMA) state.
 - You cannot use connections initiated by Junos Space Platform.
 - You cannot use the Junos OS User Interface Script Environment (JUISE).
- If you clear the **Add SNMP configuration to device** check box (on the **Modify Network Management Platform Settings** page under **Administration > Applications > Network Management Platform > Modify Application Settings**) and discover devices, and subsequently select the **Add SNMP configuration to device** check box and resynchronize nodes (**Network Monitoring > Node List > Resync Nodes**), the SNMPv2 trap target is updated on the devices.
- If you discover devices with the SNMP probing enabled, the correct version of the SNMP trap target is updated on the devices for the following cases:
 - When you modify the virtual IP (VIP) address or the device management interface IP address
 - When a separate interface for device management is configured and there is a failover of the VIP node

- When you add or delete a Fault Monitoring and Performance Monitoring (FMPM) node
- When you discover devices when the Network Monitoring service is stopped and subsequently start the Network Monitoring service and resynchronize nodes (**Network Monitoring > Node List > Resync Nodes**)

In all other cases, the default SNMP trap target (SNMPv2) is updated on the devices. If needed, you can use the predefined SNMPv3 Configlets (**CLI Configlets > CLI Configlets**) to update the trap settings on the device.

- In Junos Space Network Management Platform Release 15.1R4, Network Monitoring supports only a single set of SNMPv3 trap parameters.
- In Junos Space Network Management Platform Release 15.1R4, you cannot modify the trap settings for the SNMPv3 manager on the Network Monitoring GUI. You can modify the trap settings manually in the `/opt/opennms/etc/trapd-configuration.xml` file. After modifying the trap settings manually, restart the Network Monitoring service.
- With default SNMPv3 trap settings, the discovery of devices running worldwide Junos OS (wwJunos OS devices) fails as the default SNMPv3 trap settings cannot be updated to wwJunos OS devices because wwJunos OS devices do not support privacy settings.
- The setting to manage objects from all assigned domains can be enabled globally for all users by selecting the **Enable users to manage objects from all allowed domains in aggregated view** check box in the **Domains** section of the Modify Application Settings page (**Administration > Applications > Network Management Platform > Modify Application Settings**). Alternatively, you can enable the setting to manage objects from all assigned domains at the user level by selecting the **Manage objects from all assigned domains** check box on the **Object Visibility** tab of the Change User Settings dialog box, which appears when you click the User Settings (gear) icon on the Junos Space banner.
- The Juniper Networks Device Management Interface (DMI) schema repository (<http://xml.juniper.net/>) 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 Platform Web GUI.
 - Download the DMI schema by using an IPv4 client and update or install the DMI schema by using the Junos Space Web GUI.
- If you are planning on expanding the disk space for nodes in a Junos Space fabric (cluster) comprising of virtual appliances, you must first expand the disk space on the VIP node and ensure that the VIP node has come up (the status of the JBoss and MySQL services must be "Up") before initiating the disk expansion on the other nodes in the fabric. If you fail to do this, it might cause fabric instability and you might be unable to access to the Junos Space GUI.
- In a Junos Space fabric with two or more nodes configured with both IPv4 and IPv6 addresses (dual stack), the communications between all nodes in the fabric must be enabled for both IPv4 and IPv6 addresses.
- The Network Monitoring Topology feature is not supported on Internet Explorer.

- On a multinode setup, when you are installing more than one DMI schema, we recommend that you install one schema at a time and ensure that there is a gap of approximately two minutes between successive schema installation jobs. Scheduling schema installation jobs is a convenient way of ensuring a gap between schema installations.
- If the network connectivity at the active disaster recovery site is down and the active site cannot connect to sufficient arbiter devices after resuming network connectivity, both sites become standby disaster recovery sites. Execute the **jmp-dr manualFailover -a** command at the VIP node of the active disaster recovery site to convert the original site to the active site and start the disaster recovery process.

Changes in Default Behavior

- From Junos Space Network Management Platform Release 15.1R1 onward, the **accept-type** for the ASYNC API (`"/api/space/device-management/discover-devices?queue-url=https://{Server.ip}/api/hornet-q/queues/jms.queue.{Queue}"`) is changed to `"application/vnd.net.juniper.space.job-management.task+xml;version=1"`.
- From Junos Space Network Management Platform Release 15.1R1 onward, the **Add SNMP configuration to device** field on the Modify Application Settings page (**Administration > Applications > Network Management Platform > Modify Application Setting**) is renamed **Add SNMP configuration to device for fault monitoring**.
- From Junos Space Network Management Platform Release 15.1R1 onward, 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 UI. You can view the status of auto-resynchronization jobs from 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.

Known Behavior



CAUTION: To avoid a BEAST TLS 1.0 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. The best practice is to close your browser and relaunch it before logging in to Junos Space.

- Device-initiated connections to Junos Space may have different IP addresses from those listed in Junos Space. For example, if you use a loopback address to discover a device, you may source the SSH session of the device from its interface address (Junos OS default behavior is to select the default address) instead. This can lead to firewall conflicts.
- When a remote user with the FMPM Manager role uses the API to access Junos Space Network Management Platform, the user details are not updated in the `/opt/opennms/users.xml` file.

- You may observe the following limitations with in the Topology page:
 - The tooltip on the node displays the status as **Active/Managed** even when the node is down.
 - For an SRX Series cluster, topology links are displayed only for the primary member of the cluster and not for the secondary member.
- When unified in-service software upgrade (ISSU) is performed from the Manage Operations workflow, the Routing Engines are not rebooted. The Routing Engines must be manually rebooted for the image to be loaded.
- For LSYS (logical, nonroot) devices, when there are pending out-of-band changes on the root device, the Resolve out-of-band changes menu option is disabled for those child LSYS devices, even though Device Managed Status displays Device Changed. This is by design.
- RMA is not supported on devices running Junos OS, and devices that are not running Junos OS.
- Script Manager supports only Junos OS Release 10.x and later.
- A stage device script or image supports only devices running Junos OS Release 10.x and later.
- For unified ISSU support for both device-initiated and Junos Space-initiated dual Routing Engine connections, we strongly recommend that you configure the virtual IP (VIP) on the dual Routing Engine device. Dual Routing Engine devices without VIP configuration are not fully supported on Junos Space.
- In a single node or multiple nodes, changes to the user (for example, password, roles, and disable or enable user) take effect only at the next login.
- Looking Glass functionality is not supported on logical systems.
- If you click a chart on the Junos Space Network Management Platform user interface using Internet Explorer 8, you receive the following error message: **Statistics:I/O Error.**

Workaround:

1. Start the Registry Editor.
2. For a per-user setting, locate the following registry key:
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
 For a per-computer setting, locate the following registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
3. From the Edit menu, select **Add Value**.
 To override the directive for HTTPS connections, add the following registry value:
"BypassSSLNoCacheCheck"=Dword:00000001

To override the directive for HTTP connections, add the following registry value:
"BypassHTTPNoCacheCheck"=Dword:00000001

4. Quit the Registry Editor.

For more information, refer to <http://support.microsoft.com/kb/323308>.

- When you access the Junos Space Network Management Platform GUI from Internet Explorer 8, you cannot export and download files such as inventory details, backup configuration files, and troubleshooting logs.

Workaround:

1. Start the Registry Editor.
2. For a per-user setting, locate the following registry key:
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

For a per-computer setting, locate the following registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

3. From the Edit menu, select **Add Value**.

To override the directive for HTTPS connections, add the following registry value:
"BypassSSLNoCacheCheck"=Dword:00000001

To override the directive for HTTP connections, add the following registry value:
"BypassHTTPNoCacheCheck"=Dword:00000001

4. Quit the Registry Editor.

For more information, refer to <http://support.microsoft.com/kb/323308>.

- For devices running Junos OS Release 12.1 or later, the following parameters do not display any data in the Network Monitoring workspace because the corresponding MIB objects have been deprecated:
 - jnxJsSPUMonitoringFlowSessIPv4
 - jnxJsSPUMonitoringFlowSessIPv6
 - jnxJsSPUMonitoringCPSessIPv4
 - jnxJsSPUMonitoringCPSessIPv6
 - jnxJsNodeSessCreationPerSecIPv4
 - jnxJsNodeSessCreationPerSecIPv6
 - jnxJsNodeCurrentTotalSessIPv4
 - jnxJsNodeCurrentTotalSessIPv6

- For SNMPv3 traps, if more than one trap setting is configured in the `/opt/opennms/etc/trapd-configuration.xml` file, then the **security-name** attribute for the **snmpv3-user** element must be unique for each configuration entry. If a unique **security-name** attribute is not provided, then SNMP traps are not received by Network Monitoring.

The following is a sample snippet of the `/opt/opennms/etc/trapd-configuration.xml` file with two configuration entries:

```
<?xml version="1.0"?>
<trapd-configuration snmp-trap-port="162" new-suspect-on-trap="false">
  <snmpv3-user security-name="Space-SNMP-1" auth-passphrase="abcD123!"
auth-protocol="MD5"/>
  <snmpv3-user security-name="Space-SNMP-2" auth-passphrase="abcD123!"
auth-protocol="MD5"
  privacy-passphrase="zyxW321!" privacy-protocol="DES"/>
</trapd-configuration>
```

- When you make inventory changes in a device being managed by Junos Space Network Management Platform, acknowledge the changes (automatically or manually) and upgrade to Junos Space Network Management Platform Release 15.1R4, the User column is empty for all the acknowledged changes on the Acknowledge Inventory Changes tab of the View Inventory Changes page (on the Device Management page).
- On the **Network Monitoring > Node List > Node** page, the **ifIndex** parameter is not displayed for IPv6 interfaces if the version of Junos OS running on the device is Release 13.1 or earlier. This is because IPv6 MIBs are supported only on Junos OS Release 13.2 and later.
- When you modify the IP address of a Fault Monitoring and Performance Monitoring (FMPM) node using the Junos Space CLI, the FMPM node is displayed on the Fabric page but cannot be monitored by Junos Space Network Management Platform because of a mismatch in the certificate.

Workaround: After modifying the IP address of the FMPM node using the Junos Space CLI, generate a new certificate on the Junos Space VIP node and copy the certificate to the FMPM node by executing the following scripts on the Junos Space VIP node:

- `curl -k https://127.0.0.1:8002/cgi-bin/createCertSignReq.pl?ip='fmpm-node-ip'&user='admin'&password='password'`
- `curl -k https://127.0.0.1:8002/cgi-bin/authenticateCertification.pl?ip='fmpm-node-ip'&user='admin'&password='password'&mvCertToDestn='Y'`

where *fmpm-node-ip* is the IP address of the FMPM node and *password* is the administrator's password.

- When you execute a script and click the **View Results** link on the **Script Management Job Status** page, the details of the script execution results are displayed up to a maximum of 16,777,215 characters; the rest of the results are truncated.

This might affect users who execute the **show configuration** command on devices with large configurations or if the output of a Junos OS operational command (executed on a device) is large.

- When you configure a Junos Space fabric with dedicated database nodes, the Junos Space Platform database is moved from the Junos Space nodes to the database nodes. You cannot move the database back to the Junos Space nodes.
- 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.
- If Junos Space Network Management Platform is installed on a virtual appliance and you upgrade to Release 15.1R1 from Junos Space Platform Release 14.1R1 or earlier and try to expand the hard disk partitions, the hard disk expansion operation fails with the message **bash resize4fs: command not found**.

This issue has been fixed through PR1141669. However, if you still encounter this problem, perform the steps mentioned in the workaround.

Workaround:

1. Connect to the Junos Space node (by using SSH) and log in (as the **admin** user) to access the Junos Space CLI.
 2. Open a debug (command) prompt by using the Junos Space Settings Menu.
 3. Do one of the following:
 - If your installation of Junos Space Platform is not partitioned and only the **/** partition exists, run the following command: **resize2fs -p /dev/VolGroup00/LogVol00**
 - If your installation of Junos Space Platform contains more than one partition, do the following for each partition:
 - a. Find out the logical volume name for the partition by executing the following command: **run lvdisplay**. An example of a logical volume name for the **/var** partition is **/dev/jmpvgnocf/lvvar**.
 - b. Run the following command: **resize2fs -p logical-volume-name**
where *logical-volume-name* is the logical volume name of the partition that you obtained in the preceding step.
 4. Exit the shell prompt and the Junos Space CLI.
- 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 only accessible in the Global domain, ensure that you are in the Global domain in the most recent tab in which you are accessing the UI.

Known Issues

The following issues are still outstanding in the Junos Space Network Management Platform Release 15.1R4. For each entry, the identifier following the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

- If you assign a device to a different domain and there are dependencies, Junos Space correctly blocks the assignment but sometimes the Junos Space user interface does not display an error message. [PR1003361]
- If you modify the node management IP address (eth0) or the virtual IP address of a node using the Junos Space CLI, the IP address of the device management interface (eth3) of the node is also reset.

Workaround: Modify the node management IP address (eth0) or the Virtual IP address(eth0:0) on the **Administration > Fabric > Space Node Settings** page from the Junos Space GUI. [PR1000931]

- If you restart the Network Monitoring service from the **Administration > Applications > Manage Services** page, remote users who are currently logged in cannot access the Network Monitoring workspace. This is the default behavior if you restart the Network Monitoring service.

Workaround: Remote users should log out from the Junos Space user interface session and then log in. [PR969268]

- The remote users assigned to a domain through a remote profile are not listed on the Assigned Users tab for that domain on the Domains inventory landing page. [PR946323]
- A user with Super Administrator privileges and access to a subdomain cannot perform the Rescan Admin, Update SNMP, Schedule, and Outage actions in the Network Monitoring workspace. [PR945491]
- You may see the **Junos Space is Starting....** message on the Junos Space user interface for approximately two minutes in the following instances:
 - Uploading the CA Root Certificate or Certificate Revocation List
 - Deleting the CA Root Certificate or Certificate Revocation List
 [PR937970]

- The FMPM node contains irrelevant RPMs installed. [PR883610]
- For FMPM nodes, you cannot change the network settings using the Junos Space CLI. [PR893184]
- A user with the custom user role can view the Generated Reports page even if the View Generated Report privilege. The Generated Reports page can be viewed even if the View Generated Report privilege is not selected for a custom user role. [PR889084]

- You cannot set a domain name for a QFabric device through the Basic Setup Wizard. [PR895442]
- Group settings that are applied on the device are not displayed in the Basic Setup Wizard. [PR884068]
- When a node is set as "Inactive" in the device configuration, the Basic Setup Wizard incorrectly displays the node as "Active." [PR884074]
- The last row of the page is truncated for all generated reports. [PR889088]
- The LmSensors and UCD-SNMP MIBs should be compiled by default in Network Monitoring to monitor hardware parameters such as fan, temperature, and voltage of the Junos Space Appliance. [PR893557]
- When the VIP and Node-IP are modified using the menu options in the CLI, the devices are moved to the sync-failed state. [PR889572]
- The Internet Explorer browser may display issues such as script errors, longer response times, and slower refresh times. [PR882729]
- When the VIP address and node IP settings are modified using the Junos Space CLI, all the devices are moved into the "sync-failed" state. [PR889572]
- Device discovery fails if the tags mentioned in the CSV file are private tags in Junos Space. [PR860854]
- Although M Series, MX Series, and ACX Series devices do not support PPP as an encapsulation type, you can use the configuration editor in Junos Space Network Management Platform to configure the PPP encapsulation. [PR833612]
- Old SNMP trap targets are not removed from the device when the network settings on the Junos Space Appliance are modified. [PR689042]
- The RMA feature does not currently work for devices running Junos OS. [PR791987]
- Users without Assign/Unassign Template permissions are allowed to add templates to and delete templates from the View Assigned Shared Objects wizard. [PR816788]
- When you upgrade to Junos Space Network Management Platform Release 15.1R4, some scheduled jobs are canceled or cannot be retried if they failed. This is because job parameters may have changed in Release 15.1R4 due to bug fixes and enhancements.

Workaround: Re-create and reschedule the jobs after the upgrade to Junos Space Network Management Platform Release 15.1R4 is completed. [PR978232]

- Recurring jobs created in previous releases of Junos Space Network Management Platform Release do not run after you upgrade to Junos Space Network Management Platform Release 15.1R4.

Workaround: After the upgrade, re-create the recurring jobs on Junos Space Network Management Platform Release 15.1R4. [PR995934]

- After you upgrade to Junos Space Network Management Platform Release 15.1R4, the **Reports > Generated Reports > View/Download** page does not display reports generated using Junos Space Network Management Platform Release 13.3R1 or earlier.

Workaround: Back up previously generated reports on an external system by downloading the reports (in CSV, HTML, or PDF) *before* performing the upgrade. After the upgrade, regenerate the new reports by using the existing report definitions from the **Reports > Report Definitions** page. [PR1002281]

- On the **Device Management > Device Configuration > View/Assign Shared Objects** page, only the latest version of a previously created template can be assigned to the device. [PR1003810]
- When Junos Space Network Management Platform is configured to use remote authentication with a RADIUS server that uses Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2), the authentication fails when you enter the username in the *domain\username* format.

Workaround: Enter the username in the *domain@username* format. [PR1005943]

- The EnterpriseDefault (uei.opennms.org/generic/trap/EnterpriseDefault) event appears on the Events page in the Network Monitoring workspace only if there is no associated event definition for a received event. To create the required event definition, compile the MIB corresponding to the object ID (OID). You can find the OID by reviewing the details of the EnterpriseDefault event. For more information about compiling SNMP MIBs, refer to the [Compiling SNMP MIBs](#) topic. [PR1006133]
- When you connect to a device by using SSH, you can edit the contents of the file in the vi editor; however, only limited vi editor functionality is supported. You cannot use the left, right, up, and down arrow keys to navigate within the file, but you can use the vi editor's standard keys—H (left arrow), J (down arrow), K (up arrow), and L (right arrow). [PR1009106]
- When Junos Space Network Management Platform is configured to use remote local authentication with a RADIUS server that uses Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) and the RADIUS server is integrated with an RSA Authentication Manager Server, the Access Challenge requests between the RSA server and the RADIUS server do not work correctly.

Workaround: Use RADIUS servers configured with the Password Authentication Protocol (PAP) when you are using an RSA Authentication Manager Server. [PR1009543]

- If a report definition is created in a prior release of Junos Space Network Management Platform and a Generate Report recurring job is scheduled, the job is deprecated when you upgrade to Junos Space Network Management Platform Release 15.1R4.

Workaround: Re-create the job after you upgrade to Junos Space Network Management Platform Release 15.1R4. [PR1012568]

- On the Network Monitoring Topology page, when you clear the existing nodes in focus and click Use Default Focus (in the Node Display Warning dialog box), the names of the nodes in focus are not displayed. [PR1017453]
- When you select a category on the Topology page, log out of Junos Space and log in, the nodes in the previously selected category are added to the focus along with the category; in addition, you cannot remove the category from the focus by clicking the Remove from focus (x) button.

Workaround: To remove the category from the focus, search for and select the same category on the Topology page, and then click the Remove from focus (x) button. [PR1019193]

- Searching for IPv6 addresses using the global search feature in Junos Space Network Management Platform does not work because the colon (:) is a reserved character.

Workaround: When you are searching for IPv6 addresses, add the backslash character (\) before the colon in the IPv6 address; for example, enter 2001\:db8\:0\:0\:0\:0\:0 when you want to search for IPv6 address 2001:db8:0:0:0:0:0. [PR1010282]

- When you upgrade a cluster that contains a Junos Space node and a Fault Monitoring and Performance Monitoring (FMPM) node from Junos Space Network Management Platform Release 14.1R1 or 14.1R2 to Junos Space Platform Release 15.1R4, the Junos Space node is upgraded successfully whereas the FMPM node is not.

Before upgrading to Junos Space Network Management Platform Release 15.1R4, add the entry `\var\www\specialNodeAgent-bin\secure\swinstallSpecialNode.pl` to the `/usr/nma/lib/nmaSecurityScriptsWhitelist.rules` file in all the nodes, and then perform the upgrade. [PR1033002]

- The Network Monitoring Dashboard page does not display any information in the **Surveillance View** section of the page in the following cases:
 - A user with the FMPM Manager role and access to a subdomain logs in.
 - A user with the FMPM Read Only role and access to the global domain logs in.

Workaround: None. [PR1034280]

- If the VMWare ESX server that is used to create virtual machines (on which the Junos Space virtual appliances are deployed) is configured with a time zone other than UTC (GMT), the virtual machines consider the time configured on the ESX server as UTC time and stores the last boot time accordingly in the Linux system files. Therefore, on the Junos Space Network Management Platform GUI, the last boot time of the server that is displayed (in the Last Boot Time field on the **Administration > Fabric** page and the **Reboot Detail** tab of the View Node Detail page) is incorrect.

Workaround: Log in to the Junos Space CLI, access the shell, and set the hardware clock on the Junos Space server to the system clock (used by the Linux kernel) by executing the `hwclock --systohc` command on all nodes in the fabric. The correct last boot time is updated on the next reboot. [PR1033560]

- For devices that are discovered using device-initiated connections, the Modify Device Target (**Devices > Device Management > Device > Modify Device Target IP**) action is disabled.

Workaround: None. [PR1039316]

- If the version of Junos OS running on a device is Release 13.1 or earlier, only the IPv6 address used by Junos Space Platform to manage the device is displayed on the **Network Monitoring > Node List > Node** page; other interfaces that are configured with IPv6 addresses are not displayed.

Workaround: None. [PR1040687]

- If the version of Junos OS running on a device is Release 13.1 or earlier, when the device is discovered by using the IPv4 address, the IPv6 interfaces are not displayed on the **Network Monitoring > Node List > Node** page.

Workaround: None. [PR1041797]

- When you modify the device connection from IPv4 to IPv6 or from IPv6 to IPv4 (using the Modify Device Target IP workflow), a job is triggered and the SNMP trap target on the device is updated. However, this update is not tracked as part of the triggered job.

Workaround: None. [PR1043975]

- When you execute a local script (from the Script Management page) of the execution type **GRUPEDEXECUTION** on more than one device, the details of the job (on the Job Management page) displays the same results for all the devices being executed. [PR1044323]

- When you add or delete a Fault Monitoring and Performance Monitoring (FMPM) node, a job is triggered and the SNMP trap target on the devices are updated. However, the update process is not tracked as part of the triggered job.

Workaround: None. [PR1044827]

- When you specify SNMPv3 settings (in the `/opt/opennms/etc/trapd-configuration.xml` file) that are not supported by a Junos OS device and discover the device using SNMPv3, the device is not added to Junos Space Platform (as would be expected) and a generic error message "**Failed to configure device. Check device state**" is displayed instead of the error message from the device.

Workaround: None. [PR1044975]

- In some cases, when you deploy a Junos Space Network Management Platform open virtual appliance (OVA) image, Junos Space remains stuck in maintenance mode at 25% due to a bug in JBoss.

Workaround: Log in to the Junos Space CLI, stop the **jmp-watchdog** and **jboss** services (using the **service service-name stop** command), and then restart the **jmp-watchdog** and **jboss** services (using the **service service-name start** command). [PR1045193]

- In some cases, if a resynchronization job fails because a Junos Space node is down and you use the Archive/Purge Jobs workflow to purge all jobs, the failed resynchronization jobs are not purged. [PR1052833]
- When you deploy a device template, configlet, or device configuration to a large number of devices (more than 200), the jobs are stuck in an "In Progress" state. [PR1059995]

Workaround:

Before deploying to a large number of devices, add a **server.properties** file on Junos Space as follows:

1. Connect to the Junos Space node (by using SSH) and log in (as the **admin** user) to access the Junos Space CLI.
2. Open a debug (command) prompt by using the Junos Space Settings Menu.

3. Navigate to the `/usr/local/jboss/domain/servers/server1/` directory.
4. Create a folder named **configuration** by executing the `mkdir configuration` command.
5. Change the owner permissions of the configuration folder to `jboss:jboss` by executing the `chown jboss:jboss configuration` command.
6. Navigate to the **configuration** folder.
7. Create an empty file named **server.properties** by executing the `touch server.properties` command (or any other equivalent command).
8. Change the owner permissions of the **server.properties** file to `jboss:jboss` by executing the `chown jboss:jboss server.properties` command.
9. Use vi or any text editor to add the following lines to the **server.properties** file:

```
#Time out in milliseconds
pushConfigTimeout=600000
```
10. Save the file.
11. Exit the shell prompt and the Junos Space CLI.

- In some cases, the **Execute Operation** job displays a negative percentage completion rate. [PR1083829]
- When you attempt to compile the RFC-4802 standard MIB file in Network Monitoring using the SNMP MIB Compiler, the compilation fails even though the MIB compiled is correct.

Workaround: Copy the definition of `IANA GmplsAdminStatusInformationTC` from the **mib-IANA-GMPLS-TC-MIB.txt** file to the **mib-rfc4802.txt** file and delete `IANA GmplsAdminStatusInformationTC` from the `IMPORTS` statement of the **mib-rfc4802.txt** file as outlined in the following steps:

1. Open the **mib-IANA-GMPLS-TC-MIB.txt** file in a text editor.
2. Copy the definition of `IANA GmplsAdminStatusInformationTC` (as shown in the following paragraph) from the **mib-IANA-GMPLS-TC-MIB.txt** file.

```
IANA GmplsAdminStatusInformationTC ::= TEXTUAL-CONVENTION
    STATUS current
    DESCRIPTION
        "This data type determines the setting of the
        Admin Status flags in the Admin Status object or TLV, as
        described in RFC 3471. Setting this object to a non-zero
        value will result in the inclusion of the Admin Status
        object or TLV on signaling messages."
```

This textual convention is strongly tied to the Administrative Status Information Flags sub-registry of the GMPLS Signaling Parameters registry managed by IANA. Values should be assigned by IANA in step with the Administrative Status Flags sub-registry and using the same registry management rules. However, the actual values used in this textual convention are solely within the purview of IANA and do not necessarily match the values in the Administrative Status Information Flags sub-registry.

The definition of this textual convention with the addition of newly assigned values is published periodically by the IANA, in either the Assigned Numbers RFC, or some derivative of it specific to Internet Network Management number assignments. (The latest arrangements can be obtained by contacting the IANA.)

Requests for new values should be made to IANA via email (iana@iana.org)."

REFERENCE

- "1. Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description, RFC 3471, section 8.
2. Generalized MPLS Signaling - RSVP-TE Extensions, RFC 3473, section 7.
3. GMPLS - Communication of Alarm Information, RFC 4783, section 3.2.1."

SYNTAX BITS {

```

reflect(0), -- Reflect bit (RFC 3471)
reserved1(1), -- reserved
reserved2(2), -- reserved
reserved3(3), -- reserved
reserved4(4), -- reserved
reserved5(5), -- reserved
reserved6(6), -- reserved
reserved7(7), -- reserved
reserved8(8), -- reserved
reserved9(9), -- reserved
reserved10(10), -- reserved
reserved11(11), -- reserved
reserved12(12), -- reserved
reserved13(13), -- reserved
reserved14(14), -- reserved
reserved15(15), -- reserved
reserved16(16), -- reserved

reserved17(17), -- reserved
reserved18(18), -- reserved
reserved19(19), -- reserved
reserved20(20), -- reserved
reserved21(21), -- reserved
reserved22(22), -- reserved
reserved23(23), -- reserved
reserved24(24), -- reserved
reserved25(25), -- reserved
reserved26(26), -- reserved
reserved27(27), -- Inhibit Alarm bit (RFC 4783)
reserved28(28), -- reserved
testing(29), -- Testing bit (RFC 3473)
```

```
        administrativelyDown(30), -- Admin down (RFC 3473)
        deleteInProgress(31) -- Delete bit (RFC 3473)
    }
```

3. Open the **RFC-4802.mib** file in a text editor.
 4. Paste the definition of IANAGmplsAdminStatusInformationTC in the **RFC-4802.mib** file.
 5. Delete IANAGmplsAdminStatusInformationTC from the IMPORTS statement of the **RFC-4802.mib** file.
 6. Save the **RFC-4802.mib** file.
 7. Recompile the MIBs in Network Monitoring. [PR1065539]
- If you upgrade from Junos Space Network Management Platform Release 14.1R1 or Release 14.1R2 to Junos Space Platform Release 14.1R3 by using Internet Explorer, the upgrade status window is not displayed.
Workaround: Use Internet Explorer 10 or above when you upgrade to Junos Space Platform Release 14.1R3. [PR1087567]
 - In a Junos Space fabric configured with both IPv4 and IPv6 addresses, if you add a node using an IPv6 address, the Add Node job is completed successfully. However, the details of the Add Node job displays the IPv4 address instead of the IPv6 address.
Workaround: None. [PR1093506]
 - Information about links between devices displayed on the Network Monitoring Topology page are not displayed when you use a REST API call to view the link information.
Workaround: None. [PR1056325]
 - When you upgrade from Junos Space Platform Release 13.3 or 14.1 to Junos Space Platform Release 15.1R4, if any errors are reported in the preupgrade checks, you can fix the errors and retry the upgrade. However, when you retry the upgrade, the errors reported during the preceding upgrade are displayed temporarily for a few minutes. The correct status is displayed after a few minutes. If the correct status is not displayed, refresh the page and the correct status is displayed after the page reloads.
Workaround: None. [PR1097179]
 - When you upgrade to Junos Space Network Management Platform Release 15.1R4 and refresh the upgrade status page when the upgrade is in progress, the details of the upgrade process status are displayed. However, even if there are errors for a particular step in the upgrade, the upgrade status page still displays a green check mark against that step indicating that the step is completed.
Workaround: Check the Upgrade Status summary to find out whether errors occurred during the upgrade. [PR1097199]

- When an upgrade is in progress and if the eth0 interface of the VIP node is disconnected and the VIP node fails to switch over, the VIP address is not reachable, which means that the upgrade status cannot be viewed on the Web GUI. However, the upgrade still proceeds at the back end and the upgrade status can be viewed available when the VIP address becomes reachable.

Workaround: None. [PR1100233]

- When you restart the Network Monitoring service from the Manage Services page (**Administration > Applications > Network Management Platform**) and navigate to any Network Monitoring page after the service is successfully restarted, a pop-up message indicating that authentication is required is displayed.

Workaround: Log out of Junos Space Platform, log in again, and then access the Network Monitoring workspace. [PR1102339]

- When you create a quick template using the CLI editor and validate the configuration, in some cases the validation is not performed because of a mismatch between the DMI schema and the Junos OS CLI.

Workaround: None. [PR1103638]

- If an Enable Script, Disable Script, or Execute Script job is cancelled, the job details are not updated with the reason for the cancellation and the detailed job status (for the subjobs) does not display **Failed**. However, the job status is displayed correctly on the Job Management page.

Workaround: None. [1104701]

- When you create a report definition with the **Device Physical Inventory** report type and use **IP Address** as the filter criteria, the report is generated for all devices without the IP address filter criteria applied.

Workaround: None. [PR1109193]

- The Fabric page (**Administration > Fabric**) displays the incorrect status for a few minutes.

Workaround: Wait a few minutes for the correct status to be displayed. [PR1098184]

- If Service Now or Service Insight Release 14.1R4 or earlier is installed on Junos Space Network Management Platform Release 15.1R4, the dedicated database node functionality does not work.

Workaround: Install Service Now or Service Insight Release 15.1R1 on Junos Space Platform Release 15.1R4 to ensure that the dedicated database functionality works. [PR1110206]

- On a Junos Space fabric configured with two dedicated database nodes, if you delete the primary database node, the delete node job is completed successfully and the node is removed successfully. However, on the Fabric page, the status of the database for the existing node is displayed as **Out-of-sync**.

Workaround: None. [PR1103705]

- On a multinode setup, when you install more than one DMI schema simultaneously or within a short time span and try to create a template definition or modify the device configuration, depending on the Junos Space node that is serving the UI session, Junos

Space Platform sometimes displays an error message indicating that the schema could not be loaded or that the device configuration could not be loaded.

Workaround:

1. Find out which Junos Space node is serving the UI session.

For more information, see the *How Do I Determine Which Node in the Cluster Is Handling My Junos Space Platform UI Session?* section in the [Junos Space High Availability FAQ](#) topic.

2. Log in to the CLI of the Junos Space node that is serving the UI session and open a debug (command) prompt.
3. Execute the **service jboss restart** command to restart the JBoss service.
4. Log out of the Junos Space node.

[PR1112025]

- If you create a user and assign the capabilities (tasks) of the Job Administrator role to that user, the user cannot view the jobs of other users.

Workaround: Assign the predefined Job Administrator role to the user to ensure that the user can view the jobs of all users. [PR1113757]

- When you upgrade from Junos Space Network Platform Release 14.1 to Junos Space Platform Release 15.1R4, the progress bar (in the Software Install Status dialog box) displays **Less than 1 min left** even though the upgrade is complete.

Workaround: None. [PR1114118]

- When you schedule two or more Archive/Purge operations (on the Audit Logs page or the Jobs Management page) to run at the same time but from different domains, in some cases, the Archive/Purge operation fails.

Workaround: Schedule the Archive/Purge operation for two or more domains with a gap of at least five minutes between the operation for each domain. [PR1115245]

- The PostgreSQL process on the FMPM standby (secondary) node is not monitored.

Workaround:

1. Log in to the FMPM node (by using SSH) and open a debug (command) prompt.
2. Navigate to the **/etc/snmp/** directory.
3. Use vi or any text editor to open the **snmpd.conf** file.
4. Remove the comment tag from the **exec PostgreSQL /bin/sh /etc/snmp/moniPostgresql.sh** statement.

5. Save the **snmpd.conf** file.
6. Restart the SNMP agent on the node by executing the **service snmpd restart** command.

[PR1116414]

- If the SMTP server settings configured on Junos Space Platform (**Administration > SMTP Servers**) are incorrect and, when you generate a report, if you specify that Junos Space Platform must send the report by e-mail, the corresponding job completes successfully instead of failing. The job details display a message indicating that the report was sent by e-mail.

Workaround: Specify the correct SMTP server settings and regenerate the report.
[PR1111804]

- When you upgrade from Junos Space Platform Release 15.1R1 to Release 15.1R4 and access the Junos Space UI from a different browser session when the upgrade is in progress, the new upgrade UI (Release 15.1R1 and later) is displayed. After the upgrade is complete, the status changes to **SUCCESS**. However, the notes in the Upgrade Status Summary field displays **upgrade may not have finished or may have failed to upgrade** even though the upgrade is successful.

Workaround: None. [PR1142493]

- When you configure eth3 as the device management interface and monitor a device that is in a different subnet than that of the eth3 interface, Network Monitoring fails to monitor the device.

Workaround: Add an FMPM node and configure the eth0 interface on the FMPM node with the same information as the eth3 interface on the Junos Space node. [PR1137980]

- If Network Monitoring receives two traps within the same second, one for a trigger alarm and another for a clear alarm, then the triggered alarm is not cleared because the clear alarm is not processed by Network Monitoring.

Workaround: None. [PR1153423]

- In a disaster recovery setup that has FMPM nodes configured in a subnet other than that of the **eth0** interface, the platform upgrade image does not get copied to the slave FMPM node.

Workaround: Copy the upgrade image from **/var/cache/jboss/jmp/payloads/** in the active site to **/var/cache/jboss/jmp/payloads/** in the FMPM nodes of the standby site.
[PR1181548]

Resolved Issues

In Junos Space Network Management Platform Release 15.1R4, the issues listed in security advisory [JSA10760](#) are resolved.

Documentation Updates

This section lists the errata and changes in Junos Space Network Management Platform Release 15.1R1 documentation:

- The *High Availability Deployment Guide* is renamed *High Availability and Disaster Recovery Guide*.
- Individual guides for the Junos Space Platform workspaces are consolidated into the *Workspaces Feature Guide* to make it easier to find information.
- From Junos Space Platform Release 15.1R1 onward, a new guide called the *Complete Software Guide* (PDF only), which contains the following guides, is available:
 - *Getting Started Guide*
 - *User Interface Guide*
 - *Workspaces Feature Guide*
 - *Monitoring and Troubleshooting Guide*
 - *High Availability and Disaster Recovery Guide*
 - *Frequently Asked Questions*
- The *Junos Space Network Management Platform User Guide* is deprecated. The contents of this guide are available in the *Workspaces Feature Guide* and the *User Interface Guide*.

Junos OS Compatibility

In Junos Space Network Management Platform Release 15.1R4, no new Junos OS releases are supported. For additional information about Junos OS compatibility for Junos Space Platform Release 15.1R4, see *What Junos OS Releases Are Supported in Different Junos Space Applications?* in the [Junos Space Device Management FAQ](#) topic.

Junos Space Documentation and Release Notes

For a list of related Junos Space documentation, see <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the *Junos Space 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 <http://www.juniper.net/techpubs/>.

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for

sale at technical bookstores and book outlets around the world. The current list can be viewed at <http://www.juniper.net/books>.

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service 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 <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://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: <http://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <http://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- 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 <http://www.juniper.net/support/requesting-support.html>.

Revision History

13 Jan 2017—Revision 1

11 Oct 2017—Revision 2

Copyright © 2017 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be 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.