Junos Space Network Management Platform Release 16.1R2 Release Notes

Release 16.1R2
14 June 2017

Contents

Junos Space Network Management Platform Release Notes

These release notes accompany Junos Space Network Management Platform Release 16.1R2.

NOTE: **The terms Junos Space Network Management Platform and Junos Space Platform are used interchangeably in this document.**

Installation Instructions

Junos Space Network Management Platform Release 16.1R2 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, see the Installation and Configuration section of the JA1500 Junos Space Appliance Hardware Guide.
- For installation instructions for a JA2500 Junos Space Appliance, see the Installation and Configuration section of the JA2500 Junos Space Appliance Hardware Guide.
- For installation instructions for a Junos Space Virtual Appliance, see the Deploying the Junos Space Virtual Appliance section of the Junos Space Virtual Appliance Installation and Configuration Guide.

See "Supported Hardware" on page 8 for more information about the hardware supported.

Upgrade Instructions

This section includes instructions to upgrade to Junos Space Network Management Platform Release 16.1R2. Read these instructions before you begin the upgrade process.

In Junos Space Platform Release 16.1R2, 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 from Junos Space Platform Release 15.2R2 to Junos Space Platform Release 16.1R2 by using the Junos Space Platform UI is not supported. You must follow a multistep procedure that involves backing up data from the nodes in the Junos Space Platform setup, installing Junos Space Platform Release 16.1R2 on the nodes, and restoring backed-up data to the nodes to complete the upgrade from Junos Space Platform Release 15.2R2 to Junos Space Platform Release 16.1R2.

CAUTION: Ensure that all data on the node is backed up to a remote server before you install the Junos Space Platform Release 16.1R2 software image as part of the upgrade procedure from Junos Space Platform Release 15.2R2 to Junos Space Platform Release 16.1R2. Existing data on the node is deleted when you install Junos Space Platform Release 16.1R2.

To upgrade from Junos Space Platform Release 15.2R2 to Junos Space Platform Release 16.1R2, you must follow the procedure outlined in Upgrading to Junos Space Network Management Platform Release 16.1R1.

NOTE: The procedure described for the upgrade from Junos Space Platform Release 15.2R2 to Junos Space Platform Release 16.1R1 in Upgrading to Junos Space Network Management Platform Release 16.1R1 is also applicable for the upgrade from Junos Space Platform Release 15.2R2 to Junos Space Platform Release 16.1R2.

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
- Upgrade Notes

Instructions for Validating the Junos Space Network Management Platform OVA Image

From Junos Space Network Management Platform Release 14.1R1 onward, the Junos Space Platform open virtual appliance (OVA) image is securely signed.

NOTE:

- Validating the OVA image is optional; you can install or upgrade Junos Space Network Management Platform without validating the OVA image.
- Before you validate the OVA image, ensure that the PC on which you are performing the validation has the following utilities available: tar, openssl, and ovftool (VMWare Open Virtualization Format [OVF] Tool). You can download VMWare OVF Tool from the following location: https://my.vmware.com/web/vmware/details?productId=353&downloadGroup=OVFTOOL351 .

To validate the Junos Space Network Management Platform OVA image:

1. Download the Junos Space Platform OVA image and the Juniper Networks Root CA certificate chain file (**JuniperRootRSACA.pem**) from the Junos Space Network Management Platform - Download Software page at https://www.juniper.net/support/downloads/space.html .

   NOTE: You need to download the Juniper Networks Root CA certificate chain file only once; you can use the same file to validate OVA images for future releases of Junos Space Network Management Platform.

2. (Optional) If you downloaded the OVA image and the Root CA certificate chain file to a PC running Windows, copy the two files to a temporary directory on a PC running Linux or Unix. You can also copy the OVA image and the Root CA certificate chain file to a temporary directory (**/var/tmp** or **/tmp**) on a Junos Space node.

   NOTE: Ensure that the OVA image file and the Juniper Networks Root CA certificate chain file are not modified during the validation procedure. You can do this by providing write access to these files only to the user performing the validation procedure. This is especially important if you use a generally accessible temporary directory, such as **/tmp** or **/var/tmp**, because such directories can be accessed by several users.

3. Navigate to the directory containing the OVA image.

4. Unpack the OVA image by executing the following command:

tar xf *ova-filename*

Where *ova-filename* is the filename of the downloaded OVA image.

5. Verify that the unpacked OVA image contains a certificate chain file (**junos-space-certchain.pem**) and a signature file (**.cert** extension).

6. Validate the signature in the unpacked OVF file (extension **.ovf**) by executing the following command:

   ovftool ovf-filename

   Where *ovf-filename* is the filename of the unpacked OVF file.

7. Validate the signing certificate with the Juniper Networks Root CA certificate chain file by executing the following command:

   openssl verify -CAfile JuniperRootRSACA.pem -untrusted *Certificate-Chain-File Signature-file*

   Where **JuniperRootRSACA.pem** is the Juniper Networks Root CA certificate chain file, *Certificate-Chain-File* is the filename of the unpacked certificate chain file (extension **.pem**), and *Signature-file* is the filename of the unpacked signature file (extension **.cert)**.

   If the validation is successful, a message indicating that the validation is successful is displayed.

   A sample of the validation procedure is as follows:

```
-bash-4.1$ ls
JuniperRootRSACA.pem space-16.1R1.3.ova
-bash-4.1$ mkdir tmp
-bash-4.1$ cd tmp
-bash-4.1$ tar xf ../space-16.1R1.3.ova
-bash-4.1$ ls
junos-space-certchain.pem space-16.1R1.3.cert
space-16.1R1.3-disk1.vmdk.gz space-16.1R1.3.mf
space-16.1R1.3.ovf
-bash-4.1$ ovftool space-16.1R1.3.ovf
OVF version:   1.0
VirtualApp:    false
Name:          viso-space-16.1R1.3

Download Size:  1.76 GB

Deployment Sizes:
  Flat disks:   250.00 GB
  Sparse disks: 4.68 GB

Networks:
  Name:        VM Network
  Description: The VM Network network

Virtual Machines:
  Name:               viso-space-16.1R1.3
```

```
Operating System:   rhel5_64guest
Virtual Hardware:
  Families:         vmx-04
  Number of CPUs:   4
  Cores per socket: 1
  Memory:           8.00 GB

  Disks:
    Index:          0
    Instance ID:    7
    Capacity:       250.00 GB
    Disk Types:     SCSI-lsilogic

  NICs:
    Adapter Type:   E1000
    Connection:     VM Network

    Adapter Type:   E1000
    Connection:     VM Network

    Adapter Type:   E1000
    Connection:     VM Network

    Adapter Type:   E1000
    Connection:     VM Network
```

```
-bash-4.1$ openssl verify -CAfile JuniperRootRSACA.pem -untrusted
junos-space-certchain.pem space-16.1R1.3.cert
space-16.1R1.3.cert: OK
-bash-4.1$
```

8. (Optional) If the validation is not successful, perform the following tasks:

   a. Determine whether the contents of the OVA image are modified. If the contents are modified, download the OVA image from the Junos Space Network Management Platform - Download Software page.

   b. Determine whether the Juniper Networks Root CA certificate chain file is corrupted or modified. If it is corrupted or modified, download the Root CA certificate chain file from the Junos Space Network Management Platform - Download Software page.

   c. Retry the preceding validation steps by using one or both of the new files.

Upgrading from Prior Releases of Junos Space Network Management Platform

You can upgrade to Junos Space Network Management Platform Release 16.1R2 from the following earlier releases:

- 16.1R1

  For information about how to upgrade from Junos Space Platform Release 16.1R1 to Junos Space Platform Release 16.1R2, see Upgrading Junos Space Network Management Platform Overview and Upgrading Junos Space Network Management Platform.

- 15.2R2

For information about how to upgrade from Junos Space Platform Release 15.2R2 to Junos Space Platform Release 16.1R2, see Upgrading to Junos Space Network Management Platform Release 16.1R1.

NOTE: The procedure described for the upgrade from Junos Space Platform Release 15.2R2 to Junos Space Platform Release 16.1R1 in Upgrading to Junos Space Network Management Platform Release 16.1R1 is also applicable for the upgrade from Junos Space Platform Release 15.2R2 to Junos Space Platform Release 16.1R2.

To upgrade to Junos Space Platform Release 16.1R2 from releases earlier than Junos Space Platform Release 15.2R2, you must first upgrade to Junos Space Platform Release 15.2R2.

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.
- When you upgrade from Junos Space Platform Release 15.2R2 to Junos Space Platform Release 16.1R2, 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 UI. For detailed information about upgrading to the Junos Space Platform Release 16.1R2, see Upgrading to Junos Space Network Management Platform Release 16.1R1.
- 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, by following the procedure outlined in Upgrading to Junos Space Network Management Platform Release 16.1R1, and then reconfigure disaster recovery. For information about configuring disaster recovery, see Configuring the Disaster Recovery Process Between an Active and a Standby Site.
- After you upgrade the Junos Space Platform Release 15.2R2 setup to Junos Space Platform Release 16.1R2, all previously installed applications, except Junos Space Service Now Releases 15.1R3, 15.1R4, and 16.1R1, are disabled. You must upgrade the applications to releases that are compatible with Junos Space Platform Release 16.1R2, by using the Junos Space Platform UI.

  Service Now Release 16.1R1, that is installed on the setup before the upgrade, is enabled and ready to use after the upgrade. If Service Now Release 15.1R3 or 15.1R4 is installed on the setup before the upgrade, during the data backup procedure, you are prompted to specify whether you want to retain the specific Service Now release after the upgrade.

If you choose to retain the Service Now release, it is enabled for use after the upgrade is completed.

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.

- After you upgrade Junos Space from release 15.2 or 16.1R1 to 16.1R2, during the system log registration of a device that is discovered or connects to Junos Space, a new pattern, **"(requested 'commit synchronize' operation)"**, is added to the system log patterns on the device. When you issue a **commit synchronize** command, Junos Space Release 16.1R2 automatically resynchronizes only those devices that have the **"(requested 'commit synchronize' operation)"** pattern added to the system log patterns.

Application Compatibility

WARNING: **Before you upgrade to Junos Space Network Management Platform Release 16.1R2, 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 Platform Release 16.1R2 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:

- Network Director Release 3.0R1
- Security Director 16.1R1 and 16.2R1
- Service Insight Releases 15.1R3, 15.1R4, 16.1R1, and 16.2R1
- Service Now Releases 15.1R3, 15.1R4, 16.1R1, and 16.2R1
- 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 16.1R2 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, 5.5, or 6.0
- Kernel-based virtual machine (KVM) (Release 1.5.3-105.el7 or later) server installed on CentOS Release 7.2

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

NOTE: For information about whether a Junos Space application can be installed on a particular Junos Space Appliance (JA2500 or JA1500) or Junos Space Virtual Appliance, see the release notes of the specific Junos Space application release.

Supported Devices

No additional Juniper Networks devices are supported in Junos Space Network Management Platform Release 16.1R2.

For a list of supported devices up to and including Junos Space Platform Release 16.1R1, see Juniper Networks Devices Supported by Junos Space Network Management Platform.

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.

Junos OS Compatibility

In Junos Space Network Management Platform Release 16.1R2, no new Junos OS releases are supported. For information about Junos OS compatibility for releases up to and including Junos Space Platform Release 16.1R1, see Junos OS Releases Supported in Junos Space Network Management Platform.

New and Changed Features

- New and Changed Features in Junos Space Network Management Platform Release 16.1R2
- New and Changed Features in Junos Space Network Management Platform Release 16.1R1

New and Changed Features in Junos Space Network Management Platform Release 16.1R2

No new features are introduced in Junos Space Network Management Platform Release 16.1R2.

New and Changed Features in Junos Space Network Management Platform Release 16.1R1

This section describes new features and the enhancements to existing features in Junos Space Network Management Platform Release 16.1R1.

- **Forwarding audit logs to a system log server**—From Junos Space Network Management Platform Release 16.1R1 onward, you can forward audit logs from Junos Space Platform to a system log server. One or more criteria can be configured in Junos Space Platform based on which audit logs are selected and forwarded to system log servers. Audit logs can be forwarded using UDP, TCP, and TLSv1.2 protocols. Audit log forwarding criteria can be viewed, modified, added, deleted, and enabled or disabled. For more information, see Audit Log Forwarding in Junos Space Overview.
- **Upgrading the underlying OS to CentOS 6.8**—In Junos Space Network Management Platform Release 16.1R1, CentOS 6.8 is used as the underlying OS of the Junos Space Platform software.
- **Adding device change details to audit logs**—From Junos Space Network Management Platform Release 16.1R1 onward, you can view the details of configuration changes made to devices from the audit log entry generated for the corresponding action. You can view the device configuration changes for actions such as 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 in the Audit Log Detail dialog box. For more information, see Viewing Audit Logs.
- **Support for Open VM Tools**—From Junos Space Network Management Platform Release 16.1R1 onward, Open VM Tools are supported for use with Junos Space Virtual Appliance. Open VM Tools comprise a set of utilities that facilitate better management and enhance the performance monitoring of virtual machines in a VMware environment. For more information, see Starting Open VM Tools in Junos Space Platform.
- **Support for 192-bit and 256-bit AES encryption for the SNMP stack**—From Junos Space Platform Release 16.1R1 onward, the SNMPv3 privacy mode supports Advanced Encryption Standard (AES) algorithms with 192-bit and 256-bit encryption. This support enables you to add or query SNMP traps from devices that support only AES algorithms with 192-bit and 256-bit encryption. For more information, see Creating a Device Discovery Profile.
- **Scheduled export of device configuration to a remote server**—From Junos Space Network Management Platform Release 16.1R1 onward, you can schedule the automatic export of backed-up configuration files to a remote Secure Copy Protocol (SCP) server. For more information, see Backing Up Configuration Files.
- **Automatically disabling inactive users**—From Junos Space Network Management Platform Release 16.1R1 onward, you can use the User hyperlink on the Modify Application Settings page (**Administration > Applications > Network Management Platform > Modify Application 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.

- **Enhancements to device authentication**—From Junos Space Platform Release 16.1R1 onward, the following enhancements related to device authentication are included:
  - Support for Digital Signature Standard (DSS) and Elliptic Curve Digital Signature Algorithm (ECDSA) key algorithms to provide better security
  - Support for a key size of 4096 bits for RSA keys to provide better authentication
  - Provision to upload custom private RSA, DSS, and ECDSA keys to the Junos Space server and authenticate devices without the need to upload keys to devices from Junos Space Platform

  For more information, see Device Authentication in Junos Space Overview.
- **Support for Transport Layer Security (TLS) protocol version 1.2 algorithms and disabling of weaker algorithms during HTTPS access**—Junos Space Network Management Platform Release 16.1R1 supports TLS 1.2 algorithms for HTTPS access through Web browsers and API clients. Use the Security hyperlink on the Modify Application Settings page to disable weaker algorithms and enable TLS 1.2 algorithms in the cipher configuration of the Apache webserver. For more information, see Modifying Junos Space Network Management Platform Settings.
- **Submit workflow for CLI Configlets**—From Junos Space Platform Release 16.1 onward, you can submit configuration changes from single-execution and group-execution CLI Configlets as change requests that can be reviewed on the Review/Deploy Configuration page (Devices workspace) before being deployed to the devices.

  You can disable the submit configuration changes feature by clearing the **Enable Approval Workflow for Configlets** check box on the Modify Application Settings page. For more information, see Applying a CLI Configlet to Devices.
- **Deploying device images to primary and backup root partitions**—From Junos Space Network Management Platform Release 16.1R1 onward, device images can be deployed to both the primary and the backup root partitions of devices by selecting the **Upgrade Dual-Root Partition** check box in the **Deploy Image on Devices** dialog box. This option is available for ACX Series, EX Series, and SRX Series (SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650) devices. For more information, see Deploying Device Images.
- **Creating and managing device discovery profiles**—From Junos Space Platform Release 16.1R1 onward, you can create a device discovery profile (in the Devices workspace) to set preferences to discover devices. A device discovery profile contains device targets, probes to search devices, authentication method and details, SSH credentials, and a recurring schedule to run the device discovery profile. You can run multiple device discovery profiles to discover devices in Junos Space Platform simultaneously. For more information, see Device Discovery Profiles Overview.
- **Viewing the Device Alias custom label on the Device Management page**—From Junos Space Network Management Platform Release 16.1R1 onward, you can use the Import Customized Attributes action available on the Device Management page to import one or more custom labels and add them to one or more devices by using CSV files. You can view the predefined custom label, Device Alias, and the value assigned to it, on the Device Management page. You can also search, sort, and filter the devices on

the basis of the Device Alias custom label. For more information, see Importing Custom Labels.

- **Generating the JBoss thread dump for Junos Space nodes by using the Junos Space Platform UI**—The Generate Thread Dump action on the Fabric page of the Administration workspace enables you to generate JBoss thread dumps on Junos Space nodes, to facilitate the troubleshooting of problems with the JBoss server on the selected nodes. For more information, see Generating JBoss Thread Dump for Junos Space Nodes.
- **Configuring JBoss and OpenNMS log levels by using the Junos Space Platform UI**—The Log Configuration page in the Administration workspace enables you to configure log levels for JBoss and OpenNMS logs. For more information, see Configuring JBoss and OpenNMS Logs in Junos Space.
- **Improvements to the Domains page in the Role-Based Access Control workspace**—The improved Domains page in Junos Space Network Management Platform Release 16.1R1 supports sorting and filtering of displayed entries based on column values. The pagination controls enable you to browse through the entries and specify the number of entries to be displayed per page. For more information, see Assigning Objects to an Existing Domain.
- **Selecting the number of results in alarm and events list**—From Junos Space Network Management Platform Release 16.1R1 onward, you can select the number of results that will be displayed per page, on the alarms and events pages, up to a maximum of 1000 results. For more information, see Viewing Alarms from a Managed Device.
- **Filtering reports by domain**—From Junos Space Platform Release 16.1R1 onward, you can filter the reports available on Junos Space Network Management Platform by the domains assigned to the objects associated with the report type. For more information, see Reports Overview.
- **Additional SNMP traps for fabric monitoring**—In Junos Space Network Management Platform 16.1R1, additional SNMP traps for fabric monitoring are added and the corresponding parameters are displayed in the System Health Report under the Administration workspace. The SNMP traps are added to detect VIP binding issues, whether the fabric node is in the DOWN state, JGroups membership issues, and audit log forwarding failure. For more information, see Viewing the Administration Statistics.
- **Support for configuring Junos Space-device communication through a NAT gateway**—From Junos Space Network Management Platform Release 16.1R1 onward, you can configure and enable a Network Address Translation (NAT) server to route connections from selected or all managed devices to the Junos Space fabric from the NAT Configuration page in the Administration workspace. An updated device management configuration containing the IP addresses that are translated through NAT is configured on the devices that use the NAT server. Disable the NAT configuration when a NAT server is no longer needed to route connections. Configuring a NAT server to route connections can help you connect and manage devices that are outside or external to the Junos Space network. A new checkbox—Use NAT—is added on the Device Discovery Target page to specify whether the devices are in the external network. A new column—Device Network—is added on the Device Management page to identify whether a device uses a NAT server to route connections to Junos Space Platform. For

more information, see NAT Configuration for Junos Space Network Management Platform Overview.

You can also configure a NAT server during the initial configuration of the Junos Space Appliance or Virtual Appliance as a Junos Space node or an FMPM node.

- For more information about configuring NAT on a JA2500 Junos Space Appliance, see the *Performing Initial Configuration* section in the JA2500 Junos Space Appliance Hardware Guide.
- For more information about configuring NAT on a JA1500 Junos Space Appliance, see the *Performing Initial Configuration* section in the JA1500 Junos Space Appliance Hardware Guide.
- For more information about configuring NAT on a Junos Space Virtual Appliance, see the *Configuring the Junos Space Virtual Appliance* section in the Junos Space Virtual Appliance Installation and Configuration Guide.

Changes in Default Behavior

- From Junos Space 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 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 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.
- From Junos Space Platform Release 15.2R2 onward, Internet Explorer version 8.0 is no longer supported. Although you can access Junos Space Platform by using Internet Explorer versions 9.0 and 10.0, we recommend that you upgrade to Internet Explorer version 11.0 because it is the only version now supported by Microsoft. For more information, see https://www.microsoft.com/en-in/WindowsForBusiness/End-of-IE-support.
- From Junos Space Platform Release 16.1R1 onward, the minimum hard disk requirement for deploying a virtual appliance on a VMware ESX or ESXi server is increased from 133 GB to 250 GB.
- From Junos Space Platform Release 16.1R2 onward, validation messages are provided for tasks where CSV files are used for device selection, and all devices that are listed in the CSV file are not selected when the task is performed. Validation messages are

provided when devices are selected using CSV files from the following pages and dialog boxes:

- Deploy Device Image dialog box
- Deploy Satellite Device Image dialog box
- Stage Image on Device page
- Stage Image on Satellite Device page
- Remove Image from Staged Device dialog box
- Undeploy JAM Package from Device dialog box
- Verifying checksum of image on device(s) dialog box
- Stage Scripts on Device(s) page
- Enable Scripts on Device(s) page
- Disable Scripts on Device(s) page
- Execute Script on Device(s) page
- Remove Scripts from Device(s) dialog box
- Verify Checksum of Scripts on Device(s) dialog box

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 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 ww 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.
- 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>
```

- 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 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:

  a. **curl -k https://127.0.0.1:8002/cgi-bin/createCertSignReq.pl?ip='*fmpm-node-ip*'\&user='admin'\&password='*password*'**
  b. **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 Network Monitoring receives two traps within the same second—that is, 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.
- If you use Internet Explorer versions 8.0 or 9.0 to access the Junos Space Platform GUI, you cannot import multiple scripts or CLI Configlets at the same time.

Workaround: Use Internet Explorer Version 10.0 or later, or use a different supported browser (Mozilla Firefox or Google Chrome) to import multiple scripts or CLI Configlets at the same time.

- 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.
- 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.
- 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. see http://support.microsoft.com/kb/175500 for instructions on how 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**).
- 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, see 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 jnxSpaceHardDiskLogicalDeviceRebulding) 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.

- 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.

- 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 Platform Release 16.1R1, Network Monitoring supports only a single set of SNMPv3 trap parameters.
- In Junos Space Platform Release 16.1R1, 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.
- 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.

- When you are discovering devices running the worldwide Junos OS (ww Junos OS devices), ensure that you wait at least 10 minutes after the Add Adapter job for the device worldwide Junos adapter has completed successfully *before* triggering the device discovery.
- A new pattern **"(requested 'commit synchronize' operation)"** is added to the syslog pattern in Junos Space Release 16.1R2. During the syslog registration after a device is discovered or connects back to Junos Space following a Junos Space upgrade from release 15.2 or 16.1R1 to 16.1R2, the **"(requested 'commit synchronize' operation)"** pattern is added to the syslog patterns on the device. When you issue the **commit synchronize** command, Junos Space automatically resynchronizes only those devices that have the **"(requested 'commit synchronize' operation)"** pattern added to the syslog patterns.

Known Issues

The following issues are still outstanding in the Junos Space Network Management Platform Release 16.1R2. For each entry, the identifier following the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

- 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 ww 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]
- 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 Platform to configure the PPP encapsulation. [PR833612]
- The FMPM node contains irrelevant RPMs installed. [PR883610]
- Group settings that are applied on the device are not displayed in the Basic Setup Wizard. [PR884068]
- 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]
- 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]
- When Junos Space 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]

- In some cases, the **Execute Operation** job displays a negative percentage completion rate. [PR1083829]
- 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]
- 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?* in FAQ: Junos Space High Availability.

  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]
- 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]

- Junos Space Platform fails to purge the audit logs for the domain SYSTEM even if you select the **Purge audit logs from all accessible domains** option.

  Workaround:

  To purge audit log for the domain SYSTEM:

  1. Log in to the Junos Space Platform CLI.

  2. From the Junos Space Platform CLI, log in to the MySQL database.

  3. Run the following query in the MySQL database:

     update Auditlog set domainId=(select id from DomainEntity where name='Global') where domainId=(select id from DomainEntity where name='SYSTEM');

     This query replaces the domain name SYSTEM with Global for all audit log entries that belong to the domain SYSTEM.

  4. From the Junos Space Platform UI, go to the Audit Log ILP and verify that the domain names for all SYSTEM domain entries are set to Global.

  5. Purge the audit logs.

  [PR1158507]

- If you delete the Junos Space JBoss nodes in a fabric on which the Cassandra service is enabled and trigger a database backup, the Cassandra check box on the Database Backup page remains selected even though there are no nodes running the Cassandra service in the fabric. This causes the database backup job to fail.

  Workaround: Do one of the following:

  - When you trigger the database backup after deleting the JBoss nodes on which the Cassandra service was enabled, on the Database Backup page, clear the Cassandra check box before proceeding with the backup.
  - Before deleting the JBoss nodes with the Cassandra service enabled, disable the Cassandra service on those nodes from the Junos Space UI by right-clicking the node on the Fabric page (Administration > Fabric) and selecting the Disable Cassandra option. Then, delete the JBoss nodes and trigger the database backup. The Cassandra check box is cleared by default on the Database Backup page and you can proceed with the backup. [PR1148616]

- When you upgrade the image of a satellite device using the Deploy Satellite Device Image workflow, Junos Space Platform does not display the correct software version information for satellite devices (in the View Software Inventory page) even though the image is upgraded successfully.

  Workaround: None. [PR1162795]

- In Deploy Satellite Device Image workflow, when the "Remove the package after successful installation" is selected, the satellite software package is not deleted from the device after the installation.

  Workaround: None. [PR1164373]

- In a fabric with IPv4 and IPv6 addresses configured, if you modify the IP address of the VIP node using the Junos Space GUI (**Administration** > **Fabric** > **Space Node Settings**), then, in some cases, the Junos Space GUI is not accessible.

  Workaround:

  1. Log in to the VIP node to access the Junos Space CLI and open a debug (command) prompt.
  2. Restart the heartbeat service by using the **service heartbeat start** command.
  3. Log out of the Junos Space VIP node. [PR1178264]

- If you add X.509 parameters in the Modify Application Settings page (**Administration > Applications > Network Management Platform > Modify Application Settings > X509CertificateParameters**) and click the **Modify** button, Junos Space Platform parses the parameters from the certificate associated with users who do not have the parameters already processed. This means that users for whom the parameters were processed previously will not be processed again.

  Workaround: Do one of the following:

  - When you are adding the X.509 Certificate Parameters for the first time, ensure that you click the **Save** link to save the information and click the **Modify** button only after you have entered all the parameters.
  - If you already added the X.509 Certificate Parameters and need to modify them later, execute the **/var/www/cgi-bin/parseUserCertificates** script on the Junos Space VIP node.
  - If Junos Space Platform is not previously configured to authenticate using X.509 certificate parameters, then remove all the existing X.509 certificate parameters from the Modify Application Settings page and click the **Modify** button to remove all certificate parameters associated with users. Then, add the X.509 Certificate Parameters and click the **Modify** button, which triggers the parsing of the certificates associated with users.

  [PR1175587]

- When you install Junos Space Platform on a JA1500 or a JA2500 Junos Space Appliance by using a USB drive and the appliance boots from the USB, the menu is not displayed

properly and special characters, such as '?', appear on the menu. This issue is observed only when you use the Mac Terminal to connect to the Junos Space Appliance.

Workaround: Connect to the Junos Space Appliance by using a different terminal emulator for the Mac or by using a terminal emulator on a computer running Windows or Linux. [PR1185895]

- If a device is discovered using a custom key, you cannot execute local scripts on the device.

  Workaround: None. [PR1213430]

- When you export operations from the Operations page (using the Export Operations workflow), the options specified for the operation in the Junos Space Platform UI are not exported to the XML file.

  Workaround: None. [PR1214022]

- Junos Space Platform fails to discover a device if the device is authenticated with a custom key generated using the openssl genpkey utility and one of the following is true:

  - The key is encrypted using one of the following passphrase ciphers: des, aes128, aes256, or aes 192.
  - The key is encrypted using the ECDSA algorithm.

  Workaround: Do one of the following:

  - Use a custom key generated using the ssh-keygen utility.
  - Use a custom key generated using the openssh genpkey utility, but use DSA or RSA as the encryption algorithm.

  [PR1214215]

- In a Junos Space fabric with both eth0 and eth3 interfaces enabled and only IPv6 addresses configured, if you try to add an FMPM node (configured with both IPv4 and IPv6 addresses) using the IPv6 address, the node addition fails.

  Workaround: None. [PR1217708]

- If you are running Junos Space Platform Release 15.2R2 and managing NATted devices (devices behind NAT) using the Model Devices workflow, when you upgrade to Junos Space Platform Release 16.1R1, the Device Network field for the devices behind NAT is marked as Internal.

  Workaround: Delete the devices marked Internal and rediscover them to ensure that the Device Network field for the devices is marked correctly. [PR1219391]

- In a Junos Space fabric that includes a Cassandra node, if you try to delete a non-Cassandra node, the node deletion operation fails in some cases.

  Workaround: Do one of the following:

  - Perform the following actions:

1. Copy the **/etc/hosts** file from a Junos Space node to the Cassandra node.
2. Log in to the Cassandra node as the **admin** user and open a debug (shell) prompt.
3. Execute the **service jmp-firewall reload** command.
4. Execute the **service nma reload** command.
5. Log out of the Cassandra node.
6. Trigger the delete node operation from the Junos Space UI.

- Trigger the delete node operation from a UI session served by a Junos Space node that was added to the Junos Space fabric before the Cassandra node.

[PR1220925]

- If some external devices managed by the Junos Space fabric are down and you add a new Junos Space node to the fabric with NAT enabled, the node is added to the fabric and the Update Devices job is triggered. This job is completed successfully even though the new NAT configuration is not pushed to the devices that are down.

  Workaround: Do one of the following:

  - Ensure that all the devices are in the 'Up' state before you add a new node.
  - For the devices that are down, manually configure the **outbound-ssh** and **target-address** (SNMP trap target) configuration statements on the device.

  [PR1221595]

- If you configure a Junos Space fabric with eth0 and eth3, Junos Space Platform does not validate all the possible IP address configuration combinations.

  Workaround: Ensure that you configure the Junos Space fabric in one of the following combinations:

  - Both eth0 and eth3 configured with only the IPv4 address
  - Both eth0 and eth3 configured with IPv4 and IPv6 addresses (dual stack)

  [PR1224070]

- If some devices managed by the Junos Space fabric are down and you configure disaster recovery with NAT enabled, the disaster recovery configuration for the standby site is not pushed to the devices that are down. However, the job associated with the device updates completes successfully.

  Workaround: Do one of the following:

  - Ensure that all the devices are in the Up state before you add a new node.
  - For the devices that are down, manually configure the **outbound-ssh** and **target-address** (SNMP trap target) configuration statements on the device.

[PR1227196]

- If you configured a Junos Space fabric containing one or two dedicated database nodes and one or two FMPM nodes without configuring NAT and try to configure NAT from the Junos Space CLI of the FMPM node, the job is triggered but the configuration is not updated in the FMPM node or on the devices. In addition, if you configure NAT from the Junos Space Platform UI, the NAT configuration is updated successfully. However, the option to disable NAT is not available in the CLI of the FMPM node and the NAT configuration is shown as **NULL** in the CLI of the FMPM node.

  Workaround: For FMPM nodes, configure or disable NAT only from the Junos Space Platform UI. [PR1227595]

- If you have configured disaster recovery in your Junos Space setup and create a modeled device, the configlet generated as part of the model device creation contains only the details of the active setup and not the standby setup.

  Workaround: None. [PR1228421]

- When you try to upgrade an low-end SRX series cluster device that has the upgrade dual-root partition and ISSU/ICU options enabled, the image upgrade is executed successfully for both the nodes (node0, node1) and deployment job is successful. However, for one of the nodes (either node0 or node1), the primary partition snapshot is not copied to alternate root partition.

  Workaround: Log in to the VIP node of the SRX series cluster and execute the **request system snapshot slice alternate** command; this takes a snapshot from the primary partition and copies it to alternate partition on both nodes. [PR1228763]

- After you upgrade from Junos Space Platform Release 15.2R2 to Release 16.1R1, in some cases, you cannot modify the settings on the Modify Application Settings page.

  Workaround:

  1. Log in to the Junos Space CLI (of the VIP node) and open a debug (shell) prompt.
  2. Stop the MySQL service by executing the **service mysql stop** command.
  3. Restart the MySQL service by executing the **service mysql start** command.
  4. After the MySQL service is restarted, log out of the Junos Space CLI.

  [PR1229459]

- If you discover a device that is authenticated by using a custom key or a Junos Space key encrypted with the Digital Signature Algorithm (DSA) and try to execute a local script on the device, the script execution fails.

  Workaround: Delete the device and rediscover the device using a Junos Space key encrypted using RSA or ECDSA and execute the local script. [PR1231409]

- If you try to deploy an image on an EX Series device with the **Remove the package after successful installation** check box selected (in the **Common Deployment Options** section of the Deploy Image on Devices page), the job fails.

Workaround: None. [PR1232485]

- The authentication status of a clustered device remains as Unverified even after the SSH fingerprint of the device is acknowledged.

  Workaround: None. [PR1241912]

Resolved Issues

The following issues are resolved in Junos Space Network Management Platform Release 16.1R2. The identifier following the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

- A SLAX script that includes a parameter with the name *Password* affects the behavior of all subsequently defined parameters in the script. [PR1114844]
- When you modify the configuration of vSRX from the Modify Device Configuration page of Junos Space Platform, the protocols are not listed in the Security options. [PR1162421]
- No message is provided for devices that are not selected when a CSV file is used to select devices while performing a task. [PR1202240]
- After you upgrade to Junos Space Platform Release 15.2R2, you experience a delay of 10 through 15 seconds while selecting or switching domains. [PR1207098]
- Unable to use square brackets in CLI commands generated by Junos Space. [PR1214225]
- The MySQL database goes into the Out-of-Sync state after the second JBoss node is added to the Junos Space fabric. [PR1215640]
- In a Junos Space fabric with more than one node, you cannot upload CSV files while creating a template definition from the Junos Space Platform UI. PR[1221994]
- Jobs listed on the Job Management page cannot be filtered on the basis of the values in the Parameters column. PR[1222014]
- While deploying device images to devices with uncommitted configuration changes, the job fails with the error message, **Uncommitted changes are present in Device(s). Please perform "rollback" or "commit" in Device(s). Also use "request system reboot" command to complete the pending installation**. [PR 1232918]
- When a JBoss node is added to a Junos Space fabric, component files from Junos Space applications are not copied and synchronized to the newly added node. [PR 1233029]
- The global search feature takes a long time to display search results while searching for strings that start with the asterisk (*) character—for example, *test. [PR 1233469]
- The actual start time of scheduled jobs is constantly delayed by one minute from the scheduled start time. [PR1234926]
- Junos Space Platform stores the Autonomous System Number as -1 in the database when a device with an Autonomous System Number greater than 65535 is discovered. [PR 1235208]
- The REST call for the API GET /api/space/managed-domain/managed-elements/{id} always returns an empty response. [PR 1237709]

- The managed status of a device is displayed as Sync Failed even after the device is resynchronized multiple times. [PR 1239775]
- After the Junos Space virtual IP (VIP) failover occurs, the Junos Space Platform UI can be accessed using weak algorithms, even when the Disable weak algorithms for WEB or API access option is selected. [PR 1240952]
- The Junos Space server attempts to resolve the host loghost.example.com multiple times because of invalid configuration data in the **/etc/rsyslog.conf** file. [PR 1243622]
- The Junos Space Security Director upgrade fails after the upgrade from Junos Space Platform Release 15.2R2 to Junos Space Platform Release 16.1R1. [PR1243690]
- Certificate-based authentication fails after you upgrade a Junos Space Platform Release 15.2R2 setup to Junos Space Platform Release 16.1R1. [PR1244598]
- Login with MyCard fails. [PR 1245784]
- When Juniper Networks EX3400 devices are added to Junos Space Platform, the managed status of the devices remains in the Sync Failed state. [PR 1246987]
- When you attempt to stage a device image from Junos Space Platform, because of the nonavailability of a route through the eth3 interface, the job fails displaying an error message indicating that SCP might not be enabled. [PR1248306]
- The Add Node job fails when any of the files to be synchronized across the fabric nodes contain a space ( ) character in the filename. [PR1248319]
- When the **commit synchronize** command is executed from the device CLI, Junos Space Platform does not automatically synchronize the device. [PR1249406]
- In device-initiated connections to Junos Space Platform, too many devices remain in the CLOSE_WAIT state, causing the Junos Space server to run out of memory. [PR 1249841]
- The addition of the second JBoss node to a Junos Space fabric with one JBoss node and dedicated database nodes takes up to six hours to complete because of a corrupt NTP file on the JBoss primary node. [PR 1250278]
- The database backup file is not copied from the standby node to the active VIP node when the eth1 interface is configured on the Junos Space nodes. [PR1250720]
- The Compare Template Against Device page displays devices across domains when filters are applied on the page. [PR 1251544]
- The query of queue messages from the Hornetq after executing an EMS script does not provide all expected messages related to the script execution job.[PR1252240]
- After you upgrade from Junos Space Platform Release 15.2R2 to Junos Space Platform Release 16.1R1, existing and new users who are assigned the Super Administrator role are unable to access the Admin tab in the Network Monitoring workspace. [PR1252330]
- Load balancing among Junos Space fabric nodes is not effective when the devices are discovered through device-initiated connections. [PR1253135]
- Users without GUI access permissions can access the GUI when they log in to Junos Space Platform with the certificate parameter-based authentication mode enabled. [PR1253581]

- The server log is flooded with error messages when the certificate parameter-based authentication mode is enabled. [PR1254932]
- Device image deployment fails because of a filename pattern mismatch. [PR1256068]

Documentation Updates

This section lists the errata and changes in Junos Space Network Management Platform Release 16.1R1 documentation:

- From Junos Space Platform Release 15.2R1, the *Frequently Asked Questions* are migrated to FAQ: Junos Space Network Management Platform on the Juniper Networks TechWiki and are not available on the TechLibrary.

  The *Complete Software Guide* no longer contains the *Frequently Asked Questions*

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.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at http://www.juniper.net/techpubs/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 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: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- 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://tools.juniper.net/SerialNumberEntitlementSearch/

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

09 Mar 2017—Revision 1, Junos Space Network Management Platform Release 16.1R2

16 Mar 2017—Revision 2

31 Mar 2017—Revision 3

05 May 2017—Revision 4

14 June 2017—Revision 5