Junos Space Network Management Platform Release 17.1R1 Release Notes

Release 17.1R1
22 August 2017

Contents

Junos Space Network Management Platform Release Notes

These release notes accompany Junos Space Network Management Platform Release 17.1R1.

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 17.1R1 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 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 7 for more information about the hardware supported.

Upgrade Instructions

This section provides information about upgrading the Junos Space Network Management Platform installations running versions earlier than Release 17.1R1.

- Supported Upgrade Path
- Instructions for Validating the Junos Space Network Management Platform OVA Image
- Upgrade Notes

Supported Upgrade Path

You can upgrade Junos Space Network Management Platform installations running Release 16.1R1 or 16.1R2 to Junos Space Network Management Platform Release 17.1R1.

Junos Space Platform upgrade from Release 16.1 to 17.1 follows the standard upgrade procedure. For information about the upgrade procedure from Junos Space Platform Release 16.1 to Junos Space Platform Release 17.1, see Upgrading Junos Space Network Management Platform Overview and Upgrading Junos Space Network Management Platform.

If the Junos Space Platform installation is running a version earlier than Release 16.1, you must first upgrade the installation to Release 16.1R2 and then upgrade to Release 17.1R1. 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.

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

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.

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.
- After you upgrade from Junos Space Platform Release 16.1R1 to Junos Space Platform Release 17.1R1, delete any preexisting device image that has an **F** release number (for

example **junos-install-mx-x86-64-15.1F6-S5.6.tgz**) from the Images page and upload the image again in Junos Space Platform.

- After you upgrade Junos Space Platform to Release 17.1R1, all previously installed applications, except Junos Space Service Now are disabled. You must upgrade the applications to releases that are compatible with Junos Space Platform Release 17.1R1, by using the Junos Space Platform UI.

Application Compatibility

WARNING: **Before you upgrade to Junos Space Network Management Platform Release 17.1R1, 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 17.1R1 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 Service Director 2.1R1
- Cross Provisioning Platform 17.1R1
- Log Collector 17.1R1
- Network Director Release 3.1R1
- Security Director 17.1R1
- Service Insight Releases 15.1R3, 15.1R4, 15.1R5, 16.1R1, 16.2R1, 17.1R1, 17.2R1
- Service Now Releases 15.1R3, 15.1R4, 15.1R5, 16.1R1, 16.2R1, 17.1R1, 17.2R1
- Worldwide (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 17.1R1 can be installed on the following hardware:

- 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)

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 Junos Space Virtual Appliance, see the release notes of the specific Junos Space application release.

Supported Devices

Junos Space Network Management Platform Release 17.1R1 supports the following additional Juniper Networks devices running Junos OS:

- MX2008 3D Universal Edge Router
- QFX5110-48S Switch
- QFX5110-32Q Switch
- QFX10008 Switch
- Junos Fusion Edge

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 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 17.1R1, no new Junos OS releases are supported. For information about Junos OS compatibility for releases up to and including Junos Space Platform Release 17.1R1, see Junos OS Releases Supported in Junos Space Network Management Platform.

New and Changed Features

This section describes the new features and the enhancements to existing features in Junos Space Network Management Platform Release 17.1R1.

- **Ability to view logical interfaces across multiple devices**—From Junos Space Network Management Platform Release 17.1R1 onward, you can select multiple devices from the Device Management page to view logical interfaces on those devices. You can also execute scripts or apply CLI Configlets on multiple logical interfaces across devices. For more information, see Viewing Managed Devices.
- **Additional authentication modes for SCP server**—From Junos Space Network Management Platform Release 17.1R1 onward, you can use Junos Space key-based or custom key-based authentication to save a copy of a report or to export a backup configuration to an SCP server. Previous versions of Junos Space Platform support only password-based authentication for an SCP server. For more information, see Generating Reports and Backing Up Configuration Files.
- **Ability to select up to 200 inventory objects** —From Junos Space Network Management Platform Release 17.1R1 onward, you can select up to 200 inventory objects for actions such as applying CLI Configlets or executing scripts that require XPath processing. For more information, see Applying a CLI Configlet to Devices.
- **Autosave support for Application Settings**—From Release 17.1R1 onward, Junos Space Network Management Platform automatically saves the changes that you make in each section of the Modify Application Settings workflow. When you click **Modify** after making changes to the settings in any of the sections of the Modify Application Settings workflow, Junos Space Platform displays the summary of changes that you made and any warnings related to the changes you made. You can review the changes and confirm or cancel the changes from the **Change Summary** dialog box. For more information, see Modifying Junos Space Network Management Platform Settings.
- **Job IDs for device assignments to domains**—From Release 17.1R1 onward, Junos Space Network Management Platform generates a job ID when you assign one or more devices to a domain from the Role-Based Access Control workspace or the Device Management page. You can view the status of the job from the Job Management page. For more information, see Working with Domains.
- **Support for HTML5-based charts in Mozilla Firefox and Google Chrome**—Junos Space Network Management Platform Release 17.1R1 supports AnyChart 6.2.0 to render high-quality HTML5-based charts in Mozilla Firefox and Google Chrome browsers. However, note that Junos Space Platform continues to use Adobe Flash Player to display charts in Internet Explorer. Charts displayed in Junos Space Platform—such as Audit Log Statistical Graph, CLI Configlet Count by Device Family, Report Definition Count by User, and State of Jobs Run—use AnyChart 6.2.0. The minimum browser requirements for supporting AnyChart 6.2.0 are Internet Explorer version 11 (with Adobe Flash Player), Google Chrome version 22, and Mozilla Firefox version 27.
- **Support for cipher block chaining (CBC)**—From Release 17.1R1 onward, Junos Space Network Management Platform supports CBC mode for Advanced Encryption Standard (AES) encryption.

- **Support for user-specific idle timeout setting**—From Junos Space Platform Release 17.1R1 onward, you can specify user-specific idle timeout values when you create or modify a user account. An idle timeout value denotes a period of inactivity after which the user session expires. You can specify a value in the range of 0 through 480 minutes in the **Automatic logout after inactivity (minutes)** field of the Create User page or the Modify User page. If you set the idle timeout value to 0, the user session never expires. By default, the user-specific idle timeout value is set to the **Automatic logout after inactivity (minutes)** value configured in the User Settings section of the **Administration** > **Application Settings** page. For more information, see Configuring Users to Manage Objects in Junos Space Overview.

- **Support for Junos OS upgrade on EX Series Virtual Chassis devices**—From Junos Space Platform Release 17.1R1 onward, you can upgrade Junos OS versions running on EX Series Virtual Chassis devices from Junos Space Platform. However, upgrade of Junos OS from Junos Space Platform is not supported on EX Series mixed Virtual Chassis (MIXED-MODE-EX-VC) devices. Upgrading Junos OS from Junos Space Platform on MIXED-MODE-EX-VC devices might cause errors and fail.

- **Ability to modify SNMPv3 trap configuration from the Junos Space Platform UI**—From Junos Space Platform Release 17.1R1 onward, you can configure the SNMPv3 trap settings of the devices from the Junos Space Platform UI. The SNMPv3 trap configuration includes the username, security level, and authentication and privacy settings. Although you can configure multiple users, only the last modified user configuration is deployed onto the devices. The default username is *JunosSpace*. The security level for the JunosSpace user is set by default to *authPriv*. Modifications to SNMPv3 trap configuration trigger a restart of the OpenNMS and deployment of the new configuration onto the devices. For more information, see Managing SNMPv3 Trap Configuration.

- **Support for hardware catalog**—Starting from Release 17.1R1, Junos Space Network Management Platform supports hardware catalog that enables you to manage the addition of new hardware components such as line cards, FPCs, chassis, fan tray, and power supplies on Juniper Networks devices. When you use a hardware catalog, you do not need to update Junos Space Platform software every time a new hardware component is added to a Juniper Networks device that Junos Space Platform manages. When Juniper Networks adds new components, Juniper Networks provides a new hardware catalog that includes the information for managing the new components. You can download the new hardware catalog from Juniper Networks Subversion (SVN) Repository and import it to the Junos Space Platform. The content of the hardware catalog is derived from the latest DMI schema and always includes the latest hardware components present in the devices running Junos OS. Note that the hardware catalog does not enable fault and performance monitoring of the newly added device components. For more information, see Hardware Catalog Overview.

- **SSH fingerprint-based authentication for adding nodes to Junos Space fabric**—Starting from Junos Space Network Management Platform Release 17.1R1, when you add new nodes to the Junos Space fabric, you can optionally specify the SSH fingerprint information for the authentication and authorization of nodes. This

feature enhances the security and prevents automation attacks on the cluster through the node. For more information, see Adding a Node to an Existing Junos Space Fabric.

- **Managing missing DMI schemas**—Starting from Release 17.1R1, Junos Space Network Management Platform provides the option to update existing schemas or download missing DMI schemas from the DMI schema repository during device resynchronization. For more information, see DMI Schema Management Overview.

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

In Release 17.1, validation messages are provided for the following pages and dialog boxes, too:

- Run Operation page
- Stage Script Bundle on Devices dialog box
- Enable Script Bundle on Devices page
- Disable Script Bundle on Devices page
- Execute Script Bundle on Devices dialog box

- From Junos Space Platform Release 17.1R1 onward, the **VLAN** field in reports supports both integer and string values. Previously, the **VLAN** field in reports supported only integer values, whereas the **VLAN** field for logical interfaces accepted both integer and string values. This mismatch caused issues in displaying VLAN information for logical interfaces in reports.

  From Release 17.1R1 onward, the **VLAN** option in the **Add Filter Criteria** section of the **Create Report Definition** page and the filter support for the **VLAN** column in the **View Logical Interface** page have been removed.

- Starting from Junos Space Platform Release 16.1R2, the upgrade-related logs at **/var/jmp_upgrade** have been added to the troubleshooting logs.

- Starting with Release 17.1, Junos Space Platform boot menu accepts text inputs, such as reinstall, when you install the Junos Space Platform software from USB drives. Previously, the boot menu supported only numerical values. Now, when you do a reinstall, the software restarts and a local reboot occurs by default. Previously, you had to connect to the console and manually trigger a reboot.

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 (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.
- If you are using Internet Explorer to access the Junos Space Network Platform UI and need to copy the job ID value from the Job ID field of the Job Management page, you must click outside the job ID text to start the selection.
- After you upgrade Junos Space Platform from Release 16.1R1 to 17.1R1, the Last Reboot Reason field at **Administration** > **Fabric** > **View Node Detail** > **Reboot Detail** page shows the value as **Reboot from Shell/Other** instead of Space reboot after Software Upgrade.
- If the device IP could not be verified, the Add Unmanaged Devices action fails.

Known Issues

The following issues are still outstanding in the Junos Space Network Management Platform Release 17.1R1. 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]
- Users without Assign/Unassign Template permissions are allowed to add templates to and delete templates from the View Assigned Shared Objects wizard. [PR816788]
- Group settings that are applied on the device are not displayed in the Basic Setup Wizard. [PR884068]
- 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]
- 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]
- 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:

  - 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]

- 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]

- Network monitoring e-mail notifications show incorrect syntax without service name and SNMP details.

  Workaround: To prevent this issue, use the following formats to capture special values in the Text message field when you create e-mail notifications for events:

  ```
  ifAlias: %parm[ifAlias]%
  ifDescr: %parm[ifDescr]%
  ifName: %parm[ifName]%
  eventid: %eventid%
  severity: %severity%
  time: %time%
  notice: %noticeid%
  nodelabel: %nodelabel%
  interface: %interface%
  service: %service%
  interfaceresolve: %interfaceresolve%
  ```

  [PR1226885]

- 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]

- Junos Space Platform upgrade from Release 15.1 to 15.2 generates the following error message and fails:

  ```
  Use of uninitialized value in concatenation (.) or string at
  /var/cache/jboss/jmp/payloads/15.2R2.4/daemons/upgradeNma.pl line 402, <$fh>
  line 2.
  ```

  [PR1228049]

- When you try to upgrade a 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]

- 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]

- When you execute local scripts, the scripts run only on the VIP node in the cluster. There is no known workaround for this issue. [PR1238558]

- After the Junos Space Platform does a rescan and restarts the Network Monitoring service, the number of devices associated with a custom category (**Network Monitoring** > **Admin** > **Node Provisioning** > **Manage Surveillance Categories**) is reset to 0 (zero). There is no known workaround for this issue. [PR1238995]

- In dual-stack implementations, IPv6 virtual IP binding does not work during master node failover or after a new setup.

  Workaround: To resolve this issue, run the **service heartbeat restart** command on the master node. [PR1262104]

- Instantaneous creation of database reports fails if the time zone specified is in a format other than UTC or UTC offset. This occurs because of an OpenNMS limitation.

  Workaround: To prevent this issue, specify the time zone in the UTC+/-offset format. [PR1262239]

- DMI schemas that are listed as installed on the DMI Schemas page are missing from the file system. This problem occurs after you restore the database from the backup. There is no known workaround for this issue. [PR1263258]

- Junos Space Platform supports only Junos Space-initiated discovery of QFX devices. There is no known workaround for this issue. [PR1267622]

- OpenNMS stops updating the performance graphs. This problem occurs because Junos Space Platform that sends the SNMP requests over the interface **eth3** uses the **eth0** address as the source IP address. Because the **eth0** interface is not reachable from devices, the SNMP requests time out.

  As a workaround, you can add the following string in **/usr/sbin/jmp-firewall**:

  ETH3NET=$(ifconfig eth3 | grep 'inet addr:' | cut -d":" -f2 | cut -d" " -f1 | head -1) iptables -t nat -A POSTROUTING -p udp -o eth3 --dport 161 -j SNAT --to $ETH3NET [PR1269891]

- The Import Script and Modify Script operations fail when the script content has the special character slanted double quotation marks (“), which causes lexical errors. [PR1270670]

- If you delete a default DMI schema before you add a node, after the addition of the node, on the DMI Schema page of the Junos Space Platform UI, the deleted schema is marked as Installed but the schema remains unusable, which is because the schema is not available In the file system of the master node. In case of a cluster failover, the schemas fail to synchronize among the nodes. There is no known workaround for this issue. [PR1272125]
- Rapid increase in the size of the file **/root/dead.letter**. This problem occurs when AIDE mail notification settings are configured.

  Workaround: Disable AIDE mail notification settings. [PR1272931]
- Updating the OpenNMS keystore with custom certificates causes SSL handshake failure, and thus communication failure, between Junos Space Platform and FMPM nodes. This communication failure causes the network monitoring service to stop. There is no known workaround for this issue. [PR1273346]
- If you try to modify the configuration of a device when a DMI schema that the device uses is being installed, the modification of the device configuration fails. There is no known workaround for this issue. [PR1273620]
- If some nodes are unavailable when a DMI schema or hardware catalog is updated on Junos Space Platform, the DMI schema or hardware catalog on such nodes fails to synchronize after the nodes come back online. There is no known workaround for this issue. [PR1273937]
- The SNMPv3 trap configuration settings in the **/opt/opennms/etc/trapd-configuration.xml** file and on the managed devices are not updated after you restore the database from the backup. There is no known workaround for this issue. [PR1276974]
- Junos Space Platform does not allow you to purge jobs that are in the Pending state. There is no known workaround for this issue. [PR1279931]
- When you perform an ISSU upgrade on high-end SRX Series cluster devices, the Deploy Image job returns the **command is not valid** error and fails.

  Workaround: Instead of ISSU, perform a normal software upgrade for high-end SRX Series cluster devices. [PR1280913]
- If you abruptly terminate a browser session or a server while the modification of Application Settings is in progress, Junos Space Platform saves a copy of the running configuration as a draft configuration in the database. Even if you delete the draft configuration, Junos Space Platform creates a new draft configuration whenever you update the configuration. There is no known workaround for this issue. [PR1281485]
- If a user imports a user certificate that contains an X509 parameter value that was used in a previously imported user certificate for another user, Junos Space Platform locks both the user accounts. There is no known workaround for this issue. [PR1282190]
- Node addition fails when unicast communication is enabled on the master node. This problem occurs because the entries corresponding to the newly-added node are not updated in the initial_host configuration of domain.xml and this causes jboss initialization on the newly-added nodes to fail.

  Workaround:

To prevent this issue, you can follow this procedure while adding new nodes to a cluster if the cluster already has the first node added and the jboss communication mode changed from multicast to unicast using the script **# /var/www/cgi-bin/changeSettings2StaticIP.sh multicast2unicast** :

1. Install the required image on node 2 and add it to the cluster.
2. After the node has been added successfully, check the status of the node and confirm that all services are up on the newly-added node (Platform UI > Administration > Fabric).
3. On the primary VIP node, which is the first node added to the cluster, restart the jboss-dc service by using the **service jboss-dc restart** command.
4. Repeat these steps for each additional node that you want to add.

However, if you did not follow the preceding procedure and the node addition does not go beyond the Deploying state, follow these steps to complete the node addition:

1. On the primary VIP node, which is the first node that was added to the cluster, run the following commands to restart the jboss-dc service:

   service jboss-dc restart

2. Run the following commands to restart services on the newly-added node:

   service jmp-watchdog stop; service jboss stop; service jboss-dc stop

   service jmp-watchdog start

[1283889]

- Creation of a Quick Template using the Basic Setup fails if the Template Administrator who is creating the Quick Template does not have the Modify Configuration permission.

  Workaround: Assign Modify Configuration role to the Template Administrator account. [PR1294610]

Resolved Issues

The following issues are resolved in Junos Space Network Management Platform Release 17.1R1. The identifier following the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

- Junos Space Platform fails to flag an error when you move a cluster device to a domain other than the one the cluster belongs to or when you apply a firewall filter that is different from the one applied to the cluster to a cluster device. [PR1003361]
- SNMP configuration for CPU voltage on JA2500 devices does not work.[PR-1101473]
- Junos Space Platform shows an incorrect description for an SFP if multiple device schemas contain the same part number for an SFP. [PR1132581]
- 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. [PR1158507]

- Synchronization between Junos Space database nodes takes a long time because Junos Space Platform checks **md5sum** every time the database synchronization runs. [PR1183245]
- Junos Space Platform adds unmanaged devices without verifying the presence of such devices. [PR1202208]
- After you upgrade Junos Space Platform from Release 15.2R2, you cannot modify the settings on the Modify Application Settings page. [PR1229459]
- 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. [PR1232485]
- When there are connection issues with the database nodes, OpenNMS stops sending SNMP traps to the remote server. [PR1235571]
- The error message that Junos Space Platform returns if the HTTP request times out while a DMI schema is being downloaded does not contain any information about the error. [PR1244493]
- On Junos Space clusters that have the eth1 interface enabled, database backup files fail to synchronize across nodes. [PR1245322]
- RADIUS authentication-based login attempts to Junos Space Platform from the Security Director interface fail. [PR1246406]
- Junos Space Platform does not support key-based authentication for exporting configuration backup files to a remote server. [PR1248262]
- The Modify Application Settings option in the Junos Space Platform UI is disabled after a database restore. [PR1253165]
- When a user with permissions for the Global domain or multiple domains runs a REST API query for a device, Junos Space Platform returns either a HTTP 200 status message with no content or a 204 status even when the device is present in one of the subdomains that the user has permissions for. However, if the user has permission only for the domain or subdomian that the device is part of, the request returns the device information as expected. [PR1254032]
- The Rest API **/api/space/configuration-management/job-instances/id/apply-cli-configlet-job-results** triggers a parser error because it does not have a valid **xsd** file associated with it. [PR1254050]
- Junos Space database nodes fail to synchronize after you restore the database from a backup file. [PR1255448]
- It is not possible to view more than 100 static routes on the Security Director UI because the UI does not support navigation across pages. [PR1256633]
- Junos OS deployment on EX2200 fails as the request-package-add RPC returns NULL because of RPC timeout. [PR1259747]
- Junos Space SNMPv3 does not support special characters such as ",&, (,), \,| in passwords. [PR1261280]

- On the Network Monitoring page of the Junos Space Platform UI, the Availability and Outage fields become unresponsive while checking for the availability and outage information. This problem occurs because the **RTCD** service is disabled. [PR1261015]
- Configlet deployment fails despite successful validation of the configlet. [PR1263282]
- User sessions fail to time out after a node reboot. [PR1264421]
- Junos Space Platform does not list the image uploaded for SRX1500 in the Stage Image or Deploy Image UI for the supported device. [PR1265994]
- Policy import for a device fails as the size of the audit log generated for a firewall import exceeds the maximum size of the Detail column in the AuditLogDetail table. [PR1268525]
- Junos Space Platform returns an invalid XML file when an API call tries to retrieve the status of a failed script execution. [PR1269854]
- Junos Space Platform fails to clear certificates from the database when an attempt to create a user is canceled or aborted. This causes errors when you create new user accounts. [PR1269875]
- The **User disable mail notification** message appears frequently after a user makes changes to the **Disable inactive users after timeout** value. [PR1269988]
- It is not possible to stage or deploy minor version images to MX Series routers. [PR1271111]
- When you execute the Promote Script action on devices, you cannot set a selection value because the Selection Value list is not visible. [PR1274454]
- Network monitoring pages fail to launch after the database is restored on an eth1-enabled server. [PR1274934]
- Topology diagram developed from OSPF-based discovery does not show all connected nodes. [PR1277897]

Documentation Updates

This section lists the errata and changes in Junos Space Network Management Platform Release 17.1R1 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

20 Jul 2017—Revision 1, Junos Space Network Management Platform Release 17.1R1

24 Jul 2017—Revision 2, Added information about PRs 1294610, 1101473, and 1256158 (change in default behavior)

22 Aug 2017—Revision 3, Added information about PRs 1283889, 1272931, and 1269891