

Junos Space Network Management Platform Release 14.1R3 Release Notes

Release 14.1R3
11 November 2016

Contents

Junos Space Network Management Platform Release Notes	3
Installation Instructions	3
Upgrade Instructions	3
Instructions for Validating the Junos Space Network Management Platform OVA Image	4
Upgrading from Prior Releases of Junos Space Network Management Platform	6
Reboot Sequence After Upgrading on a Multinode Setup	6
Upgrade Notes	7
Application Compatibility	7
Supported Junos Space Applications and Adapters	7
Supported Devices	8
New and Changed Features	8
New and Changed Features in Junos Space Network Management Platform Release 14.1R3	8
New and Changed Features in Junos Space Network Management Platform Release 14.1R2	9
Operational Notes	12
Changes in Default Behavior	15
Known Behavior	16
Known Issues	21
Resolved Issues in Junos Space Network Management Platform Release 14.1R3	28
Documentation Updates	30
Junos Space High Availability Deployment Guide	30
Junos Space Network Management Platform Getting Started Guide . .	30
Junos Space Network Management Platform Online Help	30
Junos OS Compatibility	31
Junos Space Documentation and Release Notes	31

Requesting Technical Support	31
Self-Help Online Tools and Resources	32
Opening a Case with JTAC	32
Revision History	33

Junos Space Network Management Platform Release Notes

These release notes accompany Junos Space Network Management Platform Release 14.1R3.

- [Installation Instructions on page 3](#)
- [Upgrade Instructions on page 3](#)
- [Application Compatibility on page 7](#)
- [Supported Junos Space Applications and Adapters on page 7](#)
- [Supported Devices on page 8](#)
- [New and Changed Features on page 8](#)
- [Operational Notes on page 12](#)
- [Changes in Default Behavior on page 15](#)
- [Known Behavior on page 16](#)
- [Known Issues on page 21](#)
- [Resolved Issues in Junos Space Network Management Platform Release 14.1R3 on page 28](#)
- [Documentation Updates on page 30](#)
- [Junos OS Compatibility on page 31](#)

Installation Instructions

Junos Space Network Management Platform Release 14.1R3 can be installed on a Junos Space Appliance or a Junos Space Virtual Appliance.



CAUTION: During the Junos Space Network Management Platform installation process, do not modify the filename of the software image that you download from the Juniper Networks support site. If you modify the filename, the installation fails.

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

Upgrade Instructions

This section includes instructions to upgrade to Junos Space Network Management Platform Release 14.1R3. Read these instructions before you begin the upgrade process.



CAUTION: During the Junos Space Network Management Platform upgrade process, do not modify the filename of the software image that you download from the Juniper Networks support site. If you modify the filename, the upgrade fails.

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

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

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 file (**JuniperRootRSACA.pem**) from the Junos Space Network Management Platform - Download Software page at
<https://www.juniper.net/support/downloads/?p=space> .



NOTE: You need to download the Juniper Networks Root CA certificate 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 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 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 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 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 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-14.1R1.316085.ova
-bash-4.1$ mkdir tmp
-bash-4.1$ cd tmp
-bash-4.1$ tar xf ../space-14.1R1.316085.ova
-bash-4.1$ ls
junos-space-certchain.pem  space-14.1R1.316085.cert
space-14.1R1.316085-disk1.vmdk.gz  space-14.1R1.316085.mf
space-14.1R1.316085.ovf
-bash-4.1$ ovftool space-14.1R1.316085.ovf
Opening OVF source: space-14.1R1.316085.ovf
Warning: Could not verify certificate (possibly self-signed)
Warning: Not all files referred in the OVF package is accounted for in the
manifest file
OVF version: 1.0
```

Name: space-14.1R1.316085

Download Size: 1.53 GB

Deployment Sizes:

Flat disks: 32.00 GB

Sparse disks: 3.76 GB

Networks:

Name: VM Network

Description: The VM Network network

Virtual Hardware:

Family: vmx-04

Disk Types: SCSI-lsillogic

Completed successfully

```
-bash-4.1$ openssl verify -CAfile ../JuniperRootRSACA.pem -untrusted
```

```
junos-space-certchain.pem space-14.1R1.316085.cert
```

```
space-14.1R1.316085.cert: OK
```

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 file is corrupted or modified. If it is corrupted or modified, download the Root CA certificate 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 14.1R3 from the following prior versions:

- 14.1R1.9
- 14.1R2.9

Reboot Sequence After Upgrading on a Multinode Setup

When you upgrade to Junos Space Network Management Platform Release 14.1R3 on a multinode setup and initiate a reboot request, the nodes are rebooted simultaneously.

Upgrade Notes



NOTE:

- 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 starting the upgrade process, ensure that none of the nodes on the Junos Space fabric contains a large number of database backups in the `/var/cache/jboss/backup` directory. Large number of database backups may delay the initialization process. We recommend that you retain only the previous two database backups before starting the upgrade process. Delete all other database backups before starting the upgrade process.
- After the upgrade process is complete, check the status of all nodes in the Junos Space fabric (in the Administration > Fabric page) and ensure that the Status is UP for all nodes *before* you start upgrading a Junos Space application. Otherwise, the software upgrade may fail across all nodes.
- If you are upgrading a cluster (running Junos Space Network Management Platform Release 14.1R1) that contains a Junos Space node and a Fault Monitoring and Performance Monitoring (FMPM) node to Junos Space Network Management Platform Release 14.1R3, add the entry `\var\www\specialNodeAgent-bin\secure\swInstallSpecialNode.pl` to the `/usr/nma/lib/nmaSecurityScriptsWhitelist.rules` file in all the nodes *before* the upgrade, and then perform the upgrade.

Application Compatibility

Before you upgrade to Junos Space Network Management Platform Release 14.1R3, ensure that compatible versions of Junos Space applications are available for upgrade. If you upgrade to Junos Space Network Management Platform Release 14.1R3 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 2.0
- Security Director Release 14.1R2
- Service Now Release 14.1R2
- Service Insight Release 14.1R2
- Services Activation Director Release 14.3R1
- ww Junos OS Adapter

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

Supported Devices

No additional Juniper Networks devices are supported in Junos Space Network Management Platform Release 14.1R3.

For a list of supported devices for Junos Space Network Management Platform Release 14.1R1, see the FAQ topic [Which Juniper Networks Platforms Does Junos Space Network Management Platform Software Support?](#). For the list of devices supported in Junos Space Network Management Platform Release 14.1R2, refer to the [release notes](#) (PDF).



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

New and Changed Features

- [New and Changed Features in Junos Space Network Management Platform Release 14.1R3](#)
- [New and Changed Features in Junos Space Network Management Platform Release 14.1R2](#)

[New and Changed Features in Junos Space Network Management Platform Release 14.1R3](#)

This section describes new features and the enhancements to existing features in Junos Space Network Management Platform Release 14.1R3.

- **Enhancements to the Apply CLI Configlet page**—The following enhancements have been made to the **Apply CLI Configlet** page (under **CLI Configlets > Configlets**):
 - You can search for devices based on the device name.
 - You can select devices based on tags or using a comma-separated values (CSV) file.

- Pagination is added, which allows you to select devices from multiple pages.

New and Changed Features in Junos Space Network Management Platform Release 14.1R2

This section describes new features and the enhancements to existing features in Junos Space Network Management Platform Release 14.1R2.

- **Change in release numbering**—Starting from Junos Space Network Management Platform Release 14.1R1, the release numbering has changed to the *m.nRb.s* format, where *m* is the major release number, *n* is the minor release number, *b* is the build number (*b*=1 indicates an FRS release and *b*>1 indicates a maintenance release), and *s* is the (optional) spin number.
- **Support for IPv6 addresses**—Starting from Junos Space Network Management Platform Release 14.1R2, you can discover and manage devices using IPv6 addresses. Junos Space Platform supports the management of devices configured with only IPv4 addresses, only IPv6 addresses, or both. For more information, see the *Junos Space IPv6 Support Overview* topic in the “Overview” chapter (in the “Administration” part) of the [Junos Space Network Management Platform User Guide](#).

For information about how to configure IPv6 addresses, refer to the hardware documentation or the virtual appliance documentation at

http://www.juniper.net/techpubs/en_US/release-independent/junos-space/index.html

- **IPv6 addresses to manage devices**—You can input IP addresses in both IPv4 and IPv6 formats for the following device management tasks:
 - Discovering devices
 - Adding unmanaged devices
 - Creating connection profiles
 - Connecting to devices through the Secure Console
 - Uploading RSA keys to devices
- **Modifying the IP address of a device**—You can modify the IP address of a device by using the Modify Device Target IP task. You can modify IPv4 addresses and IPv6 addresses and convert IPv4 addresses to IPv6 addresses. The modified IP address configuration is not pushed to the device. Junos Space Platform verifies the modified IP address before storing it in the Junos Space Platform database.
- **Viewing IPv6 addresses**—You can view the IPv6 addresses of the devices on the following pages:
 - View Managed Devices in the Devices workspace
 - View Physical Interfaces in the Devices workspace
 - View Logical Interfaces in the Devices workspace
 - Deploy Template in the Device Templates workspace
 - Assign to Device in the Device Templates workspace

- Undeploy Template in the Device Templates workspace
- View Template Deployment in the Device Templates workspace
- Unassign from Device in the Device Templates workspace
- **API Access Profiles**—An API Access Profile restricts a Junos Space user from executing remote procedure call (RPC) commands that are potentially unsafe for or harmful to your network. An API Access Profile has multiple rules that are XPath expressions to the RPC commands that are executed. You can assign an API Access Profile to both local and remote user accounts. You assign an API Access Profile to a user or remote profile when you create or modify a user account or remote profile.
- **Fabric Node Name column**—From Junos Space Network Management Platform Release 14.1R2 onward, a new column **Fabric Node Name** on the User Sessions page displays the node to which the user is currently logged in.
- **View logged-in users by using the Junos Space CLI**—From Junos Space Network Management Platform Release 14.1R2 onward, you can use the `jmp_users` command in the Junos Space CLI to view the users logged in to the Junos Space GUI or, in other words, the Junos Space node that is serving the user. For more information, see the *Using the Junos Space CLI to View Users Logged In to the Junos Space GUI* topic in the "User Sessions" chapter (in the "Role Based Access Control" part) of the [Junos Space Network Management Platform User Guide](#).
- **Enhancements related to rebooting nodes in a Junos Space fabric**—The following enhancements are available for rebooting nodes:
 - Reason text box in the Shutdown/Reboot Node task—You can specify the reason for rebooting the nodes. Junos Space Platform also displays predefined messages for different types of reboots performed on the nodes.
 - Reboot and process details tabs in the View Node Detail pop-up window—You can view the details related to the last reboot performed on the node. You can also view the details of the processes (JBoss, Apache Webproxy, MySQL, OpenNMS, and PostgreSQL) that are currently active on the node.
- **Viewing and acknowledging inventory changes**—From the Junos Space GUI, you can view and acknowledge the inventory changes that network operators performed on devices.
- **Setting and accessing the Junos Space home page**—By default, the Junos Space Network Management Platform Dashboard page is displayed when you log in to Junos Space. From Junos Space Network Management Platform Release 14.1R2 onward, you can set a different page as the home page. The home page is displayed when you log in to Junos Space Platform. Refer to the *Junos Space Home Page Overview* topic in the "Getting Started" chapter of the [Junos Space Network Management Platform User Guide](#) for a list of pages that can be set as the Junos Space home page.
- **SNMPv3 support for collecting and forwarding Traps**—From Junos Space Network Management Platform Release 14.1R2 onward, the Network Monitoring workspace supports the collecting of performance data and receiving of traps from devices by using SNMP version 3 (SNMPv3).

- **Color-coding and dynamically updating the alarm state of services links**—The Network Monitoring Topology page provides an option to display a color-coded status of services links:
 - Green indicates that the services link is up and that no service-impacted alarm was found.
 - Red indicates that the service status is down and that a service-impacted alarm is found for that service.

When an SNMP trap is received indicating that a service-impacted alarm has changed, the services link status is dynamically updated in the topology.

- **Purging audit logs without archiving**—From Junos Space Network Management Platform Release 14.1R2 onward, you can purge audit logs without archiving them.
- **Recurring audit log archive and purge**—From Junos Space Network Management Platform Release 14.1R2 onward, you can purge audit logs (without archiving them or after archiving them) on a recurring basis using the **Recurrence** field (**Audit Logs > Audit Log > Archive/Purge Logs** page). The **Recurrence** field is enabled only if you choose to purge audit logs (without archiving them or after archiving them) older than a specified number of days.
- **Support for index page interval**—From Junos Space Network Management Platform Release 14.1R2 onward, you can specify the index page interval (in hours), which determines the interval at which Junos Space Platform reindexes objects in the database, on the **Modify Network Management Platform Settings** page (**Administration > Applications > Network Management Platform > Modify Application Settings**).
- **Viewing the job details directly from My Jobs**—From Junos Space Network Management Platform Release 14.1R2 onward, on the My Jobs dialog box (which you access by clicking the **My Jobs** icon in the Junos Space banner), you can click the job ID for a job to view the details of that job.
- **Deploying the Junos Space Virtual Appliance on a KVM server**—From Junos Space Network Management Platform Release 14.1R2 onward, you can deploy a Junos Space Virtual Appliance on a Kernel-based Virtual Machine (KVM) server (Release 0.12.1.2-2/448.el6 or later) installed on CentOS Release 6.5. For more information, see the *Deploying a Junos Space Virtual Appliance on a KVM Server* topic in the [Junos Space Virtual Appliance Deployment and Configuration Guide](#).
- **Simpler process for expanding disk partitions**—From Junos Space Network Management Platform Release 14.1R2 onward, you can select the partitions among which you want to distribute a disk resource. For example, you can distribute the disk space in a 100-GB disk among the **/**, **/var**, **/var/log**, and **/tmp** partitions of a Junos Space Virtual Appliance. For information about adding a disk resource to a Junos Space Virtual Appliance, see the *Deploying a Junos Space Virtual Appliance on an VMware ESX or VMware ESXi Server* and *Deploying a Junos Space Virtual Appliance on a KVM Server* topics in the [Junos Space Virtual Appliance Deployment and Configuration Guide](#).
- **Support for creating a unicast Junos Space cluster**—From Junos Space Network Management Platform 14.1R2 onward, you can use the **/var/www/cgi-bin/changeSettings2staticIP.sh** script to toggle between unicast and multicast traffic on the nodes of a Junos Space cluster. For more information, see the

Creating a Unicast Junos Space Cluster topic in the “Fabric” chapter (in the “Administration” part) of the [Junos Space Network Management Platform User Guide](#).

Operational Notes

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

- If you select the **Add SNMP configuration to device** check box on the **Administration > Applications > Modify Network Management Platform Settings** page and discover a device whose trap target is updated, clicking Resync Node from the Network Monitoring workspace does not reset the trap target for the device.
- If you clear the **Add SNMP configuration to device** check box on the **Administration > Applications > Modify Network Management Platform Settings** page, the trap target is not set for the device during device discovery and resynchronizing node operations.
- If you want to perform a global search by using partial keywords, append “*” to the search keywords.
- To perform a partial keyword search on tags on the Tags page (**Administration > Tags**) or the Apply Tags dialog box (right-click a device in the **Device Management** page and select **Tag It**), append * to the search keyword.
- Job Administrator privileges are required to cancel auto generated Resync Network Elements jobs.
- Internet Explorer slows down because some scripts may take an excessive amount of time to run. The browser prompts you to decide whether to continue running the slow script. Refer to <http://support.microsoft.com/kb/175500> for instructions on to fix this issue.
- When you switch from "Space as system of record" mode to "Network as system of record" mode, devices with the "Managed Status: 'Device Changed' or 'Space & Device Changed'" status are automatically synchronized after 900 seconds. To reduce this time period, modify the **Polling time period secs** setting for Network Management Platform (**Administration > Applications > Modify Application Settings**) to a lower value such as 150 seconds.
- In Space as System of Record (SSoR) mode on Junos Space, when a new authentication key is generated, devices discovered and managed using RSA keys whose management status is Device Changed move to the Key Conflict Authentication status. To resolve the conflict on the devices and bring them back to a key-based state, upload the RSA keys manually (**Devices > Upload Keys to Devices**).
- Devices such as the BX Series and MCG5000 devices that do not use system status log files are not supported in Space as System of Record (SSoR) mode.
- The **EnterpriseDefault (uei.opennms.org/generic/trap/EnterpriseDefault)** event appears on the Events page in the Network Monitoring workspace only if there is no associated event definition for a received event. To create the required event definition, compile the MIB corresponding to the object ID (OID). You can find the OID by reviewing the details of the **EnterpriseDefault** event.

For more information about compiling SNMP MIBs, refer to the [Compiling SNMP MIBs](#) topic in the *Junos Space Network Management Platform User Guide*.

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

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

- Junos Space Network Management Platform Release 14.1R3 uses OpenSSL version 0.9.8e-27.el5_10.3. Although this version is based on the older 0.9.8e branch, it contains all relevant security updates and fixes (current up to the June 2014 release) provided by OpenSSL and CentOS. For further details regarding fixes and CVEs included in this OpenSSL version, execute the following command on the Junos Space debug shell:
`rpm -q openssl-0.9.8e-27.el5_10.3 -changelog`.
- For non-SRX Series devices, device-initiated connections to Junos Space Platform that use IPv6 addresses are supported only on Junos OS Release 15.1 or later; this is because IPv6 addresses are supported in the outbound-SSH configuration only from Junos OS Release 15.1 onward for non-SRX Series devices.

For SRX Series devices, device-initiated connections to Junos Space Platform that use IPv6 addresses are supported from Junos OS Release 12.1x47D15 onward.

- Junos Space Network Management Platform Release 14.1R3 does not fully support the management of devices behind Network Address Translation (NAT). However, you can use Junos Space Platform to manage devices behind NAT (only for device-initiated connections) by using the Model/Activate Devices workflow, excluding some actions listed below, which require the IP address of the device:
 - You cannot use the network monitoring functionality.
 - You cannot use the device Web GUI.
 - You cannot use key-based authentication.

- You cannot connect to a device by using SSH.
- You cannot activate a device that is in the Return Materials Authorization (RMA) state.
- You cannot use connections initiated by Junos Space Platform.
- You cannot use the Junos OS User Interface Script Environment (JUISE).
- If you clear the **Add SNMP configuration to device** check box (on the **Modify Network Management Platform Settings** page under **Administration > Applications > Network Management Platform > Modify Application Settings**) and discover devices, and subsequently select the **Add SNMP configuration to device** check box and resynchronize nodes (**Network Monitoring > Node List > Resync Nodes**), the SNMPv2 trap target is updated on the devices.
- If you discover devices with the SNMP probing enabled, the correct version of the SNMP trap target is updated on the devices for the following cases:
 - When you modify the virtual IP (VIP) address or the device management interface IP address
 - When a separate interface for device management is configured and there is a failover of the VIP node
 - When you add or delete a Fault Monitoring and Performance Monitoring (FMPM) node
 - When you discover devices when the Network Monitoring service is stopped and subsequently start the Network Monitoring service and resynchronize nodes (**Network Monitoring > Node List > Resync Nodes**)

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

- In Junos Space Network Management Platform Release 14.1R3, Network Monitoring supports only a single set of SNMPv3 trap parameters.
- In Junos Space Network Management Platform Release 14.1R3, 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.

- If you installed the GHOST **glibc** vulnerability security patch (for more information, see <http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10671>) and upgraded to Junos Space Network Management Platform Release 14.1R3, you *do not* need to follow the previous procedure of uploading the Release 14.1R3 upgrade image using the Junos Space Web UI and running the **fixupgrade.sh** script before initiating the upgrade to Release 14.1R3. In Junos Space Network Management Platform Release 14.1R3, the upgrade script includes the **fixupgrade.sh** script and automatically executes the script when you upgrade.

Changes in Default Behavior

- From Junos Space Network Management Platform Release 14.1R1 onward, on the Fabric page, the application logic status of Junos Space nodes is shown as UP only after all the Enterprise Archive (EAR) files for the Junos Space node are deployed and the schemas are processed. [PR951985]
- From Junos Space Network Management Platform Release 14.1R1 onward, the name of the sample comma-separated values (CSV) file downloaded from the Images and Scripts workspace is changed to **DeviceSelectSample.csv**. [PR1002481]
- From Junos Space Network Management Platform Release 14.1R1 onward, the **Linkd** menu item on the **View** menu on the Network Monitoring Topology page is renamed to **EnLinkd**.
- From Junos Space Network Management Platform Release 14.1R1 onward, the SNMP polling time for discovering links between devices is set using the **rescan_interval** parameter in the **Enhancedlink.xml** file. In prior releases, this SNMP polling time for discovering links between devices was set using the **snmp_polling** parameter in the **linkd.xml** file. The default value for the **rescan_interval** parameter is 86,400,000 milliseconds
- From Junos Space Network Management Platform Release 14.1R1 onward, changes have been made to the following Network Monitoring Topology layouts:
 - D3 layout—This layout is added.
 - ISOM layout, KK layout, and Spring layout—These layouts are deprecated.
 - FR layout—This layout is modified.
- From Junos Space Network Management Platform Release 14.1R2 onward, you can add, modify, or delete surveillance categories on the Surveillance Categories page (**Network Monitoring > Admin > Manage Surveillance Categories**).
- From Junos Space Network Management Platform 14.1R3 onward, there is no restriction on applying CLI Configlets only to the first 1000 devices displayed on the **Apply CLI Configlets** page.

Known Behavior



CAUTION: To avoid a BEAST TLS 1.0 attack, whenever you log in to Junos Space through a browser tab or window, make sure that the tab or window was not previously used to access a non-HTTPS website. The best practice is to close your browser and relaunch it before logging in to Junos Space.

- Device-initiated connections to Junos Space may have different IP addresses from those listed in Junos Space. For example, if you use a loopback address to discover a device, you may source the SSH session of the device from its interface address (Junos OS default behavior is to select the default address) instead. This can lead to firewall conflicts.
- When a remote user with the FMPM Manager role uses the API to access Junos Space Network Management Platform, the user details are not updated in the `/opt/opennms/users.xml` file.
- You may observe the following limitations with in the Topology page:
 - The tooltip on the node displays the status as **Active/Managed** even when the node is down.
 - For an SRX Series cluster, topology links are displayed only for the primary member of the cluster and not for the secondary member.
- When unified in-service software upgrade (ISSU) is performed from the Manage Operations workflow, the Routing Engines are not rebooted. The Routing Engines must be manually rebooted for the image to be loaded.
- For LSYS (logical, nonroot) devices, when there are pending out-of-band changes on the root device, the Resolve out-of-band changes menu option is disabled for those child LSYS devices, even though Device Managed Status displays Device Changed. This is by design.
- RMA is not supported on devices running 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.

- If you click a chart on the Junos Space Network Management Platform user interface using Internet Explorer 8, you receive the following error message: **Statistics:I/O Error**.

Workaround:

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

For a per-computer setting, locate the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

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

To override the directive for HTTPS connections, add the following registry value:

"BypassSSLNoCacheCheck"=Dword:00000001

To override the directive for HTTP connections, add the following registry value:

"BypassHTTPNoCacheCheck"=Dword:00000001

4. Quit the Registry Editor.

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

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

Workaround:

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

For a per-computer setting, locate the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

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

To override the directive for HTTPS connections, add the following registry value:

"BypassSSLNoCacheCheck"=Dword:00000001

To override the directive for HTTP connections, add the following registry value:

"BypassHTTPNoCacheCheck"=Dword:00000001

4. Quit Registry Editor.

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

- For devices running Junos OS Release 12.1 or later, the following parameters do not display any data in the Network Monitoring workspace because the corresponding MIB objects have been deprecated:

- jnxJsSPUMonitoringFlowSessIPv4
 - jnxJsSPUMonitoringFlowSessIPv6
 - jnxJsSPUMonitoringCPSessIPv4
 - jnxJsSPUMonitoringCPSessIPv6
 - jnxJsNodeSessCreationPerSecIPv4
 - jnxJsNodeSessCreationPerSecIPv6
 - jnxJsNodeCurrentTotalSessIPv4
 - jnxJsNodeCurrentTotalSessIPv6
- For SNMPv3 traps, if more than one trap setting is configured in the `/opt/opennms/etc/trapd-configuration.xml` file, then the **security-name** attribute for the **snmpv3-user** element must be unique for each configuration entry. If a unique **security-name** attribute is not provided, then SNMP traps are not received by Network Monitoring.

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

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

- When you make inventory changes in a device being managed by Junos Space Network Management Platform, acknowledge the changes (automatically or manually) and upgrade to Junos Space Network Management Platform Release 14.1R2, the User column is empty for all the acknowledged changes on the Acknowledge Inventory Changes tab of the View Inventory Changes page (on the Device Management page).
- On the **Network Monitoring > Node List > Node** page, the **ifIndex** parameter is not displayed for IPv6 interfaces if the version of Junos OS running on the device is Release 13.1 or earlier. This is because IPv6 MIBs are supported only on Junos OS Release 13.2 and later.
- For devices discovered using SNMPv3 with only authentication enabled, the near real-time (NRT) graphs (under **Network Monitoring > Reports > Resource Graphs**) are blank.

Workaround: Modify the SNMPv3 polling parameters (to enable both authentication and privacy) for the existing devices (on the **Network Monitoring > Admin > Configure SNMP Community Names by IP** page) and run the **Update SNMP** action from the **Network Monitoring > Node List > Node** page.

- When you modify the IP address of a Fault Monitoring and Performance Monitoring (FMPM) node using the Junos Space CLI, the FMPM node is displayed on the Fabric page but cannot be monitored by Junos Space Network Management Platform because of a mismatch in the certificate.

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

- 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.

- If you perform an in-service software upgrade (ISSU) on a device running Junos OS (by using Junos Space Network Management Platform Release 14.1R2 or earlier) and if the SSH connection between the device and Junos Space is broken, after the SSH connection is re-established, the ISSU on the device is not completed. This issue has been fixed via PR1073499. However, if you still encounter this problem, perform the steps mentioned in the workaround.

Workaround:

Before performing the ISSU by using Junos Space, add a **server.properties** file on Junos Space as follows:

1. Connect to the Junos Space node (by using SSH) and log in (as the **admin** user) to access the Junos Space CLI.
2. Open a debug (command) prompt by using the Junos Space Settings Menu.
3. Navigate to the `/usr/local/jboss/domain/servers/server1/` directory.
4. Create a folder named **configuration** by executing the `mkdir configuration` command.
5. Change the owner permissions of the configuration folder to `jboss:jboss` by executing the `chown jboss:jboss configuration` command.
6. Navigate to the **configuration** folder.
7. Create an empty file named **server.properties** by executing the `touch server.properties` command (or any other equivalent command).
8. Change the owner permissions of the **server.properties** file to `jboss:jboss` by executing the `chown jboss:jboss server.properties` command.
9. Use vi or any text editor to add the following lines to the **server.properties** file:


```
device-upgrade-reconnect-time=upgrade-reconnect-time-in-milliseconds
device-reboot-connect-wait-time=reboot-connect-wait-time-in-milliseconds
device-reboot-connect-retry-count=reboot-connect-retry-count
device-upgrade-reconnect-retry-count=upgrade-reconnect-retry-count
```



NOTE: An explanation of these parameters is as follows:

- **device-reboot-connect-wait-time**—Indicates the time (in milliseconds) that Junos Space waits for a device to come up and reconnect to Junos Space after a reboot is triggered on a device. The default is 1 minute (60000 milliseconds).
- **device-reboot-connect-retry-count**—After Junos Space waits for the configured **device-reboot-connect-wait-time**, it sends a **get-system-info** Remote Procedure Call (RPC) to the device to confirm the reconnection. This parameter specifies the number of times that Junos Space sends the RPC to the device. The default is 30 attempts.

The total time that Junos Space waits for a device to reconnect is equal to the product of the **device-reboot-connect-wait-time** and the **device-reboot-connect-retry-count**.

- **device-upgrade-reconnect-retry-count**—During an ISSU triggered by Junos Space, when the mastership switchover occurs and a device disconnects from Junos Space, this parameter specifies the number of attempts that Junos Space makes to check if the new master has connected to Junos Space. If the device is still connected to the old master (because the mastership switchover is not complete), then Junos Space disconnects the device connection and tries again. The default number of attempts is 45 and the time interval between successive attempts is approximately 1 minute.

You can set this parameter to a higher value to accommodate slower devices that take longer for the mastership switchover to occur and then reconnect.

- **device-upgrade-reconnect-time**—During an ISSU triggered by Junos Space, when the mastership switchover occurs and a device disconnects from Junos Space, this parameter controls the time (in milliseconds) that Junos Space waits (the first time) for the device to reconnect. If the device fails to connect back within this time, then the ISSU is marked as failed. If the device connects, then Junos Space continues to check if the new master has connected (the number of attempts depends on the configured **device-upgrade-reconnect-retry-count**). The default is 900000 milliseconds (15 minutes).

10. Save the file.

11. Exit the shell prompt and the Junos Space CLI, and retry the ISSU procedure.

Known Issues

The following issues are still outstanding in the Junos Space Network Management Platform Release 14.1R2. For each entry, the identifier following the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

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

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

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

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

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

- You cannot filter the device templates by the **Deployment Status** column on the Templates page. [PR938517]
- Filters are not enabled on the Staged Images and Deploy Images page. You cannot filter these pages to view the devices on which the software is already staged. [PR932442]
- You receive an email from ?root@host? from the disaster recovery setup. [PR919436]

Workaround: Move the **mcelog.cron** file from the **/etc/cron.hourly** directory to the **/var/tmp** directory. This stops the notification.

- The FMPM node contains irrelevant RPMs installed. [PR883610]

- For FMPM nodes, you cannot change the network settings using the Junos Space CLI. [PR893184]
- A user with the custom user role can view the Generated Reports page even if the View Generated Report privilege. The Generated Reports page can be viewed even if the View Generated Report privilege is not selected for a custom user role. [PR889084]
- You cannot set a domain name for a QFabric device through the Basic Setup Wizard. [PR895442]
- Group settings that are applied on the device are not displayed in the Basic Setup Wizard. [PR884068]
- When a node is set as “Inactive” in the device configuration, the Basic Setup Wizard incorrectly displays the node as “Active.” [PR884074]
- The last row of the page is truncated for all generated reports. [PR889088]
- The LmSensors and UCD-SNMP MIBs should be compiled by default in Network Monitoring to monitor hardware parameters such as fan, temperature, and voltage of the Junos Space Appliance. [PR893557]
- When the VIP and Node-IP are modified using the menu options in the CLI, the devices are moved to the sync-failed state. [PR889572]
- The Internet Explorer browser may display issues such as script errors, longer response times, and slower refresh times. [PR882729]
- When the VIP address and node IP settings are modified using the Junos Space CLI, all the devices are moved into the “sync-failed” state. [PR889572]
- Unified ISSU support or CLI-command modification is needed from TXP-3D. [PR880614]
- Device discovery fails if the tags mentioned in the CSV file are private tags in Junos Space. [PR860854]
- Although M Series, MX Series, and ACX Series devices do not support PPP as an encapsulation type, you can use the configuration editor in Junos Space Network Management Platform to configure the PPP encapsulation. [PR833612]
- Old SNMP trap targets are not removed from the device when the network settings on the Junos Space Appliance are modified. [PR689042]
- The RMA feature does not currently work for devices running Junos OS. [PR791987]
- Users without Assign/Unassign Template permissions are allowed to add templates to and delete templates from the View Assigned Shared Objects wizard. [PR816788]
- Changes made to the candidate configurations in prior releases of Junos Space Network Management Platform are discarded when you upgrade to Junos Space Network Management Platform Release 14.1R2.

Workaround: Deploy all configuration changes made through the candidate configuration on the **Review/Deploy Configuration** page (under **Devices > Device Management**) before upgrading to Junos Space Network Management Platform Release 14.1R2. [PR887739]

- When you upgrade to Junos Space Network Management Platform Release 14.1R2, some scheduled jobs are canceled or cannot be retried if they failed. This is because job parameters may have changed in Release 14.1R2 due to bug fixes and enhancements.

Workaround: Re-create and reschedule the jobs after the upgrade to Junos Space Network Management Platform Release 14.1R2 is completed. [PR978232]

- Recurring jobs created in previous releases of Junos Space Network Management Platform Release do not run after you upgrade to Junos Space Network Management Platform Release 14.1R2.

Workaround: After the upgrade, re-create the recurring jobs on Junos Space Network Management Platform Release 14.1R2. [PR995934]

- After you upgrade to Junos Space Network Management Platform Release 14.1R2, the **Reports > Generated Reports > View/Download** page does not display reports generated using Junos Space Network Management Platform Release 13.3R1 or earlier.

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

- On the **Device Management > Device Configuration > View/Assign Shared Objects** page, only the latest version of a previously created template can be assigned to the device. [PR1003810]

- When Junos Space Network Management Platform is configured to use remote authentication with a RADIUS server that uses Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2), the authentication fails when you enter the username in the *domain\username* format.

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

- The EnterpriseDefault (uei.opennms.org/generic/trap/EnterpriseDefault) event appears on the Events page in the Network Monitoring workspace only if there is no associated event definition for a received event. To create the required event definition, compile the MIB corresponding to the object ID (OID). You can find the OID by reviewing the details of the EnterpriseDefault event. For more information about compiling SNMP MIBs, refer to the [Compiling SNMP MIBs](#) topic in the *Junos Space Network Management Platform User Guide*. [PR1006133]

- When you connect to a device by using SSH, you can edit the contents of the file in the vi editor; however, only limited vi editor functionality is supported. You cannot use the left, right, up, and down arrow keys to navigate within the file, but you can use the vi editor's standard keys—H (left arrow), J (down arrow), K (up arrow), and L (right arrow). [PR1009106]

- When Junos Space Network Management Platform is configured to use remote local authentication with a RADIUS server that uses Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) and the RADIUS server is integrated with an RSA Authentication Manager Server, the Access Challenge requests between the RSA server and the RADIUS server do not work correctly.

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

- Though Firefly devices are displayed on the Network Monitoring Topology page, the links between such devices are not displayed. [PR1011207]
- In the Network Monitoring Topology page, the display of bridge links between devices is not supported. [PR1011230]
- If a report definitions is created in a prior release of Junos Space Network Management Platform and a Generate Report recurring job is scheduled, the job is deprecated when you upgrade to Junos Space Network Management Platform Release 14.1R3.

Workaround: Re-create the job you upgrade to Junos Space Network Management Platform Release 14.1R3. [PR1012568]

- On the Network Monitoring Topology page, when you clear the existing nodes in focus and click Use Default Focus (in the Node Display Warning dialog box), the names of the nodes in focus are not displayed. [PR1017453]
- In some cases, when you use Mozilla Firefox version 31.0 to access the Junos Space GUI, the Junos Space Login page does not load. This issue has been observed on PCs running both Mac OS X and Microsoft Windows. (For more information about this issue, refer to the following links on the Mozilla Firefox Support website:
<https://support.mozilla.org/en-US/questions/1012728#answer-616338> and
<https://support.mozilla.org/en-US/questions/1012765>.)

Workaround:



NOTE: The following steps are for Mozilla Firefox version 31.0 running on Microsoft Windows; the procedure for Mac OS X might differ.

1. On the Mozilla Firefox menu bar, click **Tools** and select **Options**.
The Options dialog box is displayed.
2. Click the **Advanced** icon and then select the **Certificates** tab.
3. Click **View Certificates**.
The Certificate Manager dialog box is displayed.
4. Select the **Authorities** tab.
5. On the **Authorities** tab, select the entries for one or more Junos Space Platform virtual IP (VIP) addresses that you are unable to access in Firefox.
6. Click **Delete or Distrust**.
A dialog box lists the previously selected entries.
7. Click **OK**.
The entries that you selected are deleted.

8. Click **OK** in the Certificate Manager dialog box, and then click **OK** in the Options dialog box.
9. (Optional) Restart Firefox.
10. In the Mozilla Firefox address bar, type the VIP address that you want to access.
You should now be able to access the Junos Space Login page.

[PR1017999]

- When you select a category on the Topology page, log out of Junos Space and log in, the nodes in the previously selected category are added to the focus along with the category; in addition, you cannot remove the category from the focus by clicking the Remove from focus (x) button.

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

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

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

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

Before upgrading to Junos Space Network Management Platform Release 14.1R2, add the entry `\var\www\specialNodeAgent-bin\secure\swinstallSpecialNode.pl` to the `/usr/nma/lib/nmaSecurityScriptsWhitelist.rules` file in all the nodes, and then perform the upgrade. [PR1033002]

- For worldwide Junos OS (wwJunos OS) devices, the Modify Device Target (**Devices > Device Management > Device > Modify Device Target IP**) action is disabled.

Workaround: None. [PR1034088]

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

Workaround: None. [PR1034280]

- If the VMWare ESX server that is used to create virtual machines (on which the Junos Space virtual appliances are deployed) is configured with a time zone other than UTC (GMT), the virtual machines consider the time configured on the ESX server as UTC time and stores the last boot time accordingly in the Linux system files. Therefore, on the Junos Space Network Management Platform GUI, the last boot time of the server

that is displayed (in the Last Boot Time field on the **Administration > Fabric** page and the **Reboot Detail** tab of the View Node Detail page) is incorrect.

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

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

Workaround: None. [PR1039316]

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

Workaround: None. [PR1040687]

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

Workaround: None. [PR1041797]

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

Workaround: None. [PR1043975]

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

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

Workaround: None. [PR1044827]

- When you specify SNMPv3 settings (in the **/opt/opennms/etc/trapd-configuration.xml** file) that are not supported by a Junos OS device and discover the device using SNMPv3, the device discovery job runs successfully and the SNMPv2 trap target is updated on the device.

Workaround: None. [PR1044975]

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

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

- Jobs related to schema installation are not purged by Junos Space Platform. [PR1048567]
- In some cases, if a resynchronization job fails because a Junos Space node is down and you use the Archive/Purge Jobs workflow to purge all jobs, the failed resynchronization jobs are not purged. [PR1052833]
- When you deploy a device template, configlet, or device configuration to a large number of devices (more than 200), the jobs are stuck in an "In Progress" state. [PR1059995]

Workaround:

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

1. Connect to the Junos Space node (by using SSH) and log in (as the **admin** user) to access the Junos Space CLI.
 2. Open a debug (command) prompt by using the Junos Space Settings Menu.
 3. Navigate to the **/usr/local/jboss/domain/servers/server1/** directory.
 4. Create a folder named **configuration** by executing the **mkdir configuration** command.
 5. Change the owner permissions of the configuration folder to jboss:jboss by executing the **chown jboss:jboss configuration** command.
 6. Navigate to the **configuration** folder.
 7. Create an empty file named **server.properties** by executing the **touch server.properties** command (or any other equivalent command).
 8. Change the owner permissions of the **server.properties** file to jboss:jboss by executing the **chown jboss:jboss server.properties** command.
 9. Use vi or any text editor to add the following lines to the **server.properties** file:


```
#Time out in milliseconds
pushConfigTimeout=600000
```
 10. Save the file.
 11. Exit the shell prompt and the Junos Space CLI.
- In some cases, the **Execute Operation** job displays a negative percentage completion rate. [PR1083829]
 - When you attempt to compile the RFC-4802 standard MIB file in Network Monitoring using the SNMP MIB Compiler, the compilation fails even though the MIB compiled is correct.

Workaround:

1. Open the **RFC-4802.mib** file in a text editor.
 2. Remove the line that contains "DEFVAL { { } })".
 3. Save the **RFC-4802.mib** file.
 4. Recompile the MIBs in Network Monitoring. [PR1065539]
- When you upgrade an IPv6-enabled installation of Junos Space Network Management Platform (that has two nodes in the fabric) from Release 14.1R2 to Release 14.1R3, the upgrade fails if the two nodes are configured with both IPv4 and IPv6 addresses and the IPv4 address of each node has an identical numerical value to the corresponding last four hexets of the IPv6 address configured for the other node.

For example, if the first node has the addresses 10.208.135.77 (IPv4) and 2001:db8:0:1:10:208:135:78 (IPv6) configured for the eth0 interface, and the second node has the addresses 10.208.135.78 (IPv4) and 2001:db8:0:1:10:208:135:77 (IPv6) configured for the eth0 interface, the IPv4 address configured for the first node is numerically identical to the last 4 hexets of the IPv6 address configured for the second node and the IPv4 address configured for the second node is numerically identical to the last four hexets of the IPv6 address configured for the first node; in such a case, the upgrade from Junos Space Network Management Platform Release 14.1R2 to Release 14.1R3 fails.

Workaround: Ensure that the IPv4 address of each node does not have an identical numerical value to the corresponding last four hexets of the IPv6 address configured for the other node. Alternatively, perform the upgrade with only IPv4 addresses configured and configure the IPv6 addresses after upgrading to Junos Space Network Management Platform Release 14.1R3. [PR1083855]

- If you upgrade from Junos Space Network Management Platform Release 14.1R1 or Release 14.1R2 to Junos Space Platform Release 14.1R3 by using Internet Explorer, the upgrade status window is not displayed.

Workaround: Use Internet Explorer 10 or above when you upgrade to Junos Space Platform Release 14.1R3. [PR1087567]

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

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

Resolved Issues in Junos Space Network Management Platform Release 14.1R3

The following issues are resolved in Junos Space Network Management Platform Release 14.1R3. The identifier following the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

- Archiving and purging a large number of jobs (greater than 30,000) fails. [PR1036423]
- When you create a quick template (by using the CLI-based Template Editor) with the device family as MX Series and the version as Junos OS 12.3R1.7, Junos Space Network

Management Platform displays error messages when some CLI commands are included in the quick template. [PR1059764]

- When hundreds of devices are managed by Junos Space Network Management Platform and you try to generate a “Device Physical Inventory” report, the report generation fails. [PR1060208]
- On a Junos Space fabric with Network Monitoring enabled on an FMPM node, the database backup fails. [PR1060325]
- If the connection status of a device managed by Junos Space Platform is “Down” and a manual resynchronization is performed, Junos Space Platform pushes an incorrect configuration to the device and performs a commit operation. [PR1061674]
- When you upgrade a Junos Space fabric with two or more nodes, the overall system condition gauge on the Dashboard page incorrectly displays Average instead of Good. [PR1062335]
- On the Operation Result Detail page, the status of the operation is not displayed. [PR1063147]
- If you configure Junos Space Platform to use remote authentication or remote local authentication using a RADIUS server or a TACACS+ server but do not configure a remote profile for the user on Junos Space Platform, the user is unable to log in to Junos Space Platform even though the user is configured locally on Junos Space Platform. [PR1065500]
- Audit logs deleted on Junos Space Platform are not cleaned up from the database, which causes Junos Space to go out of memory. [PR1071624]
- On the Run Operation page, if you select devices based on several tags and execute the operation, Junos Space Network Management Platform fails to create the job. [PR1071647]
- A device running Junos OS 14.1X* (for example, 14.1X53-D10) that is discovered by Junos Space Platform using a device-initiated connection cannot connect to Junos Space Platform in the following cases: after Junos Space is rebooted, after the device is rebooted, or whenever the SSH connection between the device and Junos Space Platform is broken. [PR1072091]
- When you create a quick template (using the CLI-based template editor) for an SRX Series device running Junos OS Release 11.* or Release 12.*, the quick template does not save some CLI commands. [PR1073558]
- If you try to apply a CLI Configlet that contains the value * in the configuration on MX Series devices, the operation fails. [PR1075478]
- After upgrading to Junos Space Network Management Platform Release 14.1R2, the template and CLI Configlet search does not work. [PR1075494]
- If you try to apply a CLI Configlet that contains the value * in the configuration on a device, the operation fails. [PR1076070]

- When you choose devices by using tags and execute an operation, the operation is executed on devices that are not selected. [PR1076502]
- When the network is the system of record (NSOR mode) and a device connection (to Junos Space Platform) is reestablished, even if the device configuration state was "In Sync" before the disconnection, the device configuration state initially changes from "In Sync" to "Out of sync" regardless of whether the configuration time stamp matches or not. [PR 1079172]

Documentation Updates

This section lists the errata and changes in Junos Space Network Management Platform Release 14.1R3 documentation:

- [Junos Space High Availability Deployment Guide](#)
- [Junos Space Network Management Platform Getting Started Guide](#)
- [Junos Space Network Management Platform Online Help](#)

Junos Space High Availability Deployment Guide

- In the *Junos Space High Availability Overview* topic, it is mentioned that the virtual appliance can be deployed on a VMware ESX server. From Junos Space Network Management Platform Release 14.1R2 onward, the virtual appliance can also be deployed on a Kernel-based Virtual Machine (KVM) server.
- In the *Configuring the Junos Space Cluster for High Availability Overview* topic, it is mentioned that the virtual appliance can be deployed on VMware ESX server 4.0 or later or VMware ESXi server 4.0, 5.0, 5.1, or 5.5. From Junos Space Network Management Platform Release 14.1R2 onward, you can also deploy a virtual appliance on a KVM server (Release 0.12.1.2-2/448.el6 or later) installed on CentOS Release 6.5. For more information, see the *Deploying a Junos Space Virtual Appliance on a KVM Server* topic in the [Junos Space Virtual Appliance Deployment and Configuration Guide](#)

Junos Space Network Management Platform Getting Started Guide

- In the "Basic Requirements for a Fabric Deployment" section of the *Junos Space Fabric Deployment Overview* topic, it is mentioned that if you are deploying a fabric of virtual appliances, we recommend that the first and the second appliance added to the fabric are hosted on separate VMware ESX/ESXi servers to ensure failover support. From Junos Space Network Management Platform Release 14.1R2 onward, you can also host the first and second appliance added to the fabric on separate KVM servers.

Junos Space Network Management Platform Online Help

- The *Fabric Management Overview* topic includes an incorrect link to the Junos Space Appliance and Junos Space Virtual Appliance documentation. The correct link is http://www.juniper.net/techpubs/en_US/release-independent/junos-space/index.html.
- The *Upgrading Junos Space Network Management Platform* topic includes incorrect information about upgrade paths. Refer to the [Upgrading from Prior Releases of Junos Space Network Management Platform on page 6](#) section for the correct information.

- The *Upgrading Junos Space Software Overview* topic contains information about Junos Space Network Management Platform Release 13.3R1. Refer to the *Upgrading Junos Space Software Overview* topic in the *Junos Space Network Management Platform User Guide* for the correct information.

Junos OS Compatibility

In Junos Space Network Management Platform Release 14.1R2, support for Junos OS Release 14.2 was added. For additional information on the Junos OS compatibility information, see the FAQ topic [What Junos Releases Are Supported in Different Junos Space Applications](#).

Related Documentation

- *Junos® Space 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>.

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

14 May 2015—Revision 1, Junos Space Network Management Platform Release 14.1R3

19 Jun 2015—Revision 2

15 January 2016—Revision 3

13 June 2016—Revision 4

11 November 2016—Revision 5

Copyright © 2016, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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