Release Notes

Published
2025-06-19

release-note-23.1R1

Table of Contents

Introduction

Junos Space is a comprehensive network management solution that simplifies and automates management of Juniper Networks switching, routing, and firewall.

Junos Space Management Applications optimize network management by extending the breadth of the Junos Space solution for various domains in service provider and enterprise environments.

These release notes accompany Junos Space Network Management Platform Release 23.1R1.

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

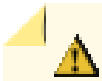
New and Changed Features

Junos Space® Network Management Platform Release 23.1R1 supports the following enhancement:

- Support for TLS 1.2 with SMTP— Starting in Junos Space Network Management Platform 23.1R1, we've provided TLS 1.2 SMTP email support.
- Disaster Recovery (DR) improvements— Starting in Junos Space Network Management Platform 23.1R1, we've provided the following enhancements:
  - DR improvements for MySQL replications, PostgreSQL replications, and automatic failover.
  - Autorecovery of devices in case of errors during replication process or with dr-watchdog, and other services.
  - Seamless functioning of the DR without manual intervention after a delay in the back up of the standby site.

Installation Instructions

Junos Space Network Management Platform Release 23.1R1 can be installed on 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 Junos Space Virtual Appliance, see the Junos Space Virtual Appliance Deployment Overview section of the Junos Space Virtual Appliance Installation and Configuration Guide.

See "Supported Hardware" on page 10 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 23.1R1.

- "Supported Upgrade Path" on page 2
- "Upgrade Notes" on page 4
- "Instructions for Validating the Junos Space Network Management Platform OVA Image" on page 6

Supported Upgrade Path

Table 1 on page 3 provides information about the supported upgrade path across Junos Space Network Management Platform releases.

Table 1: Supported Upgrade Path

Upgrade from Junos Space Release	Upgrade to Junos Space Release										
Junos Space Release	19.3	19.4	20.1	20.3	21.1	21.2	21.3	22.1	22.2	22.3	23.1
19.1	Yes										
19.2	Yes	Yes									
19.3		Yes	Yes	Yes							
19.4			Yes	Yes							
20.1				Yes							
20.3					Yes						
21.1						Yes	Yes				
21.2							Yes	Yes			
21.3								Yes	Yes		
22.1									Yes	Yes	
22.2										Yes	Yes
22.3											Yes

Related Information

- Upgrading Junos Space Network Management Platform Overview
- Juniper Networks Devices Supported by Junos Space Network Management Platform
- Upgrading Junos Space Network Management Platform

NOTE: Before you upgrade Junos Space Platform to Release 23.1, ensure that the time on all Junos Space nodes is synchronized. For information about synchronizing time on Junos Space nodes, see Synchronizing Time Across Junos Space Nodes.

You can upgrade to Junos Space Network Management Platform 23.1R1 from the following earlier releases:

- Junos Space Network Management Platform Release 22.3R1
- Junos Space Network Management Platform Release 22.2R1

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.

Upgrade Notes

IMPORTANT:

- In Junos Space Network Management Platform Release 22.2R1 hot patch v5, the **systemd-python** package is installed for the fail2ban service. When you upgrade from Junos Space Network Management Platform Release 22.2R1 hot patch v5 to Junos Space Network Management Platform Release 23.1R1, the following error occurs:

  ```
  Failed dependencies:
        systemd = 219-78.el7 is needed by (installed) systemd-python-219-78.el7.x86_64
        systemd-libs = 219-78.el7 is needed by (installed) systemd-
  python-219-78.el7.x86_64
  ```

  Workaround—Before upgrading from Junos Space Network Management Platform Release 22.2R1 hot patch v5 to Junos Space Network Management Platform Release 23.1R1, use `# yum remove systemd-python` command to uninstall the library before upgrading to Junos Space Network Management Platform Release 23.1R1.

- In case, you try to remove the **systemd-python** package using rpm -e systemd-python or yum remove systemd-python, you might receive the following error:

  ```
  Failed dependencies:
      systemd-python is needed by (installed) fail2ban-server-0.11.2-3.el7.noarch
  ```

  Workaround—Perform the steps to remove all fail2ban RPMs:

  1. Use the following commands:

     ```
     rpm -e fail2ban-firewalld-0.11.2-3.el7.noarch \
            fail2ban-server-0.11.2-3.el7.noarch \
            fail2ban-0.11.2-3.el7.noarch \
            fail2ban-sendmail-0.11.2-3.el7.noarch
     ```

  2. Remove the **systemd-python** package by using rpm -e systemd-python-219-78.el7.x86_64 command.

- 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.
- To upgrade to Junos Space Network Management Platform Release 23.1, follow the procedure mentioned in Upgrading Junos Space Network Management Platform.
- 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.
- After you upgrade Junos Space Platform to Release 23.1R1, all previously installed applications are disabled until the applications are upgraded to a version compatible with Junos Space Platform 23.1R1. You must upgrade the applications to releases that are compatible with Junos Space Platform Release 23.1R1, by using the Junos Space Platform UI. For information about application versions compatible with Junos Space Platform 23.1R1, see "Application Compatibility" on page 9.

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 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/downloads/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.

Management Scalability

We recommend the following API limit for Junos Space Network Management Platform and Security Director:

- RAM: 64 GB
- CPU Cores: 8
- No. of API calls per minutes: 500
- Response size: ~ 500 KB

NOTE: NOTE: The number of successful API calls and time taken to execute might vary based on the response payload. Extremely large payloads will slow down request completion process. The size of the response you receive from an API might differ based on the endpoint you call. Different endpoints return varying amounts of data depending on their intended functionality and purpose.

Application Compatibility

WARNING: Before you upgrade to Junos Space Network Management Platform Release 23.1R1, ensure that compatible versions of Junos Space applications are available for upgrade by referring to the Junos Space Application Compatibility Junos Space Application Compatibility knowledge base article. If you upgrade to Junos Space Platform Release 23.1R1 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 release a compatible version of the Junos Space application.

This release of Junos Space Network Management Platform supports Worldwide (ww) Junos OS Adapter adapter and the following applications.

- Security Director 23.1R1
- Network Director 7.1R1

Supported Hardware

Junos Space Network Management Platform Release 23.1R1 can be installed on the following hardware:

- VMware ESXi server 6.7 and 7.0

  NOTE: Adobe Flash is no longer supported and VMware ESXi server 6.0 and 6.5 are removed.

- Kernel-based virtual machine (KVM) (Release 1.5.3-141.el7_4.4 or later)

NOTE: Starting in Junos Space Network Management Platform Release 22.1R1 onward, we do not support installation on JA2500 Junos Space appliance.

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

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

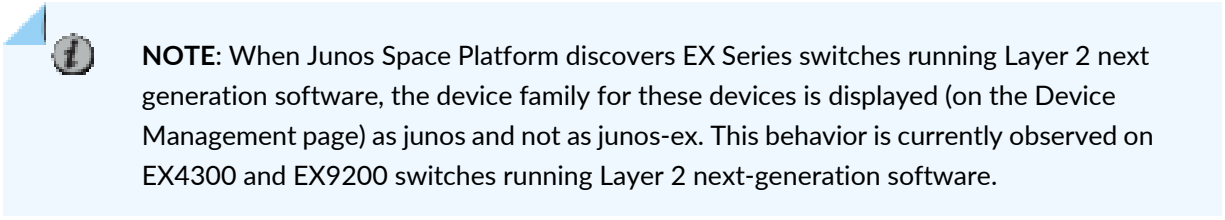
NOTE: For detailed information about hardware requirements, see Junos Space Virtual Appliance Deployment Overview.

Supported Devices

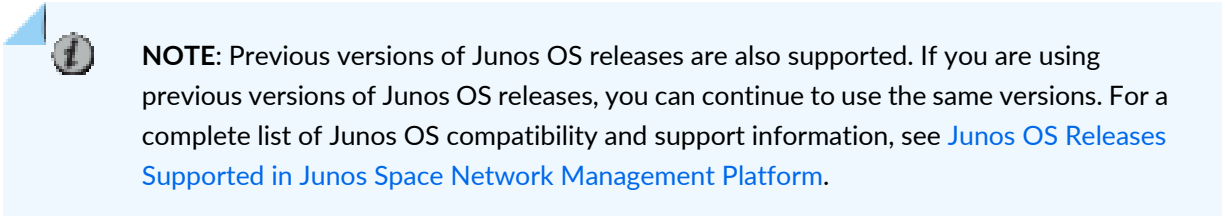
Junos Space Network Management Platform Release 23.1R1 supports the following additional Juniper Networks device and components running Junos OS:

- EX4100-24P
- EX4100-24T
- EX4100-24MP
- EX4100-F-24P
- EX4100-48P
- EX4400-24X

For a list of supported devices up to and including Junos Space Platform Release 23.1R1, 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.



NOTE: Previous versions of Junos OS releases are also supported. If you are using previous versions of Junos OS releases, you can continue to use the same versions. For a complete list of Junos OS compatibility and support information, see Junos OS Releases Supported in Junos Space Network Management Platform.

Changes in Default Behavior

- From Release 17.2R1 onward, Junos Space Platform does not sort configurations while comparing templates. In releases earlier than 17.2R1, Junos Space Platform sorts configurations while comparing templates, and this causes Junos Space Platform to trigger incorrect deviation reports because of a change in the order of configuration statements caused by the sorting.

- From Release 17.2R1 onward, Junos Space Platform does not support the click action in the Top 10 Active Users in 24 Hours chart. In releases earlier than 17.2R1, you can click within the chart to view details of the selected item on the corresponding page.
- From Junos Space Platform Release 17.1R1 onward, the VLAN field in reports supports both integer and string values. In releases earlier than 17.1R1, the VLAN field in reports supports only integer values, whereas the VLAN field for logical interfaces accepts both integer and string values. This mismatch causes 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 on the View Logical Interface page are removed.
- From Junos Space Platform Release 16.1R2 onward, the upgrade-related logs at **/var/jmp_upgrade** are added to the troubleshooting logs.
- From Release 17.1R1 onward, Junos Space Platform boot menu accepts text inputs, such as reinstall, when you install the Junos Space Platform software from USB drives. In versions earlier than Release 17.1R1, the boot menu supports only numerical values. From Release 17.1R1 onward, 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.
- 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
  - 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

  From Release 17.1R1 onward, 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

- Starting in Junos Space Network Management Platform Release 21.3R1, unicast Junos Space cluster is the default mode for Junos Space Network Management Platform.
- Starting in Junos Space Network Management Platform Release 21.3R1, the AppLogic node restarts, when the Add Node jobs for JBoss and database nodes are successful. This is not applicable for Fault Monitoring and Performance Monitoring (FMPM) node.
- While upgrading from Junos Space Network Management Platform Release 21.1R1 (with Junos Space Network Management Platform Release 21.1R1 supported applications) or Junos Space Network Management Platform Release 21.2R1 (with Junos Space Network Management Platform Release 21.1R1 supported applications) to Junos Space Network Management Platform Release 21.3R1, the deployment status is displayed only for the Junos Space Network Management Platform and not for the applications.
- Starting in Junos Space Network Management Platform Release 21.3R1, the scripts with existing Network Configuration protocol (NETCONF) Remote Procedure Calls (RPC) commands needs to be replaced with CLI commands with display xml option.
- Starting in Junos Space Network Management Platform Release 21.3R1, the AppLogic service restarts after the application upgrade or installation job is successful.
- Starting in Junos Space Network Management Platform Release 21.3R1, before initiating any operation like configuration change, configlet or template push to the device, make sure that the nodes are not in Deploying / Parsing Schema state.

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.

- For EX Series Switches, an explicit reboot is required, using the device CLI to complete the image deployment and upgrade process.
- Starting from Junos Space Network Management Platform Release 18.1R1 onwards, to view and edit firewall policies, users must have permissions or roles corresponding to all the attributes present under the Firewall Policies and Shared Objects predefined roles. Go to Network Management Platform>Role Based Access Control>Roles to view and assign the relevant roles.
- Tag names can be alphanumeric strings. The tag name can also contain underscores, hyphens, and spaces. However, a tag name must not:
  - Exceed 255 characters
  - Start with a space
  - Contain special characters such as commas, double quotation marks, or parentheses.

  NOTE: “Untagged” is a reserved term and, therefore, you cannot create a tag with this name.
- The right-click menu is not available on the Import Licenses (Administration > Licenses > Import License) page. You can use either the browser menu options or the keyboard shortcuts to copy and paste onto the page.
- Device-initiated connections to Junos Space can have different IP addresses from those listed in Junos Space. For example, if you use a loopback address to discover a device, you can 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/etc/users.xml** file.
- You might observe the following limitations on 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:

  1. curl -k https://127.0.0.1:8002/cgi-bin/createCertSignReq.pl? ip='fmpm-node-ip'\&user='admin'\&password='password'
  2. 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 rests 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 on the Device Management page and select Tag It), append * to the search keyword.

- Internet Explorer slows down because some scripts can 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 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 Compiling SNMP MIBs.

- When a physical hard drive is removed from a Junos Space hardware appliance 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.

- 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 (Configlets CLI) 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 (https://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 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 on the 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

This section lists the known issues in Junos Space Network Management Platform Release 23.1R1.

For the most complete and latest information about known defects, use the Juniper Networks online Junos Problem Report Search application.

- During the Disaster Recovery (DR) initialization process, when you try to retrieve information for all the arbiter devices, it fails with an error. PR1702232
- Validation issue with device selection disables the NEXT button. PR1668786

Resolved Issues

For the most complete and latest information about known defects, use the Juniper Networks online Junos Problem Report Search application.

- While reading the inventory file, an automatic resync caused by the configlets or hardware changes gets stuck for twelve minutes. PR1648325
- Junos Space Network Management Platform modifies or deletes SNMPv3 configurations from devices. PR1664169
- The purging policy provided in Junos Space Network Management Platform, fails to remove the database backup files even when the purge job is complete. PR1686226
- DR setup fails to start due to MySQL replication issue. PR1689277
- Junos Space Network Management Platform shows images as staged even when they are not. PR1693261
- Some of the logical system (LSYS) devices show as down when the root device is up. PR1699230
- RESTAPI stops working with exception `null value for userName or passwd.` PR1700218
- Junos-es devices contains match term GRES, which matches with the words INGRESS and EGRESS causing unnecessary load in the traffic logs. PR1701653
- On the Junos Space Network Management Platform GUI, the Script Verification Results page displays a maximum of 200 devices even when the user has more than 200 devices. PR1705251
- The managed status of a device continues to remain out-of-sync even when the device is up again. PR1710003

- There is an issue with synchronization between Junos Space Network Management Platform and the SRX340 device. PR1711201
- User receives the CLI password expiration warning much earlier than expected. PR1714872
- The Quick template editor is unable to retain the comments when you save the changes. PR1719821
- User is unable to receive Junos Space Fabric Monitoring alerts in all the configured emails, but only in one email. PR1723041
- Error while trying to synchronize the OpenNMS files through **sync.sh**. PR1694579

Hot Patch Releases

This section describes the installation procedure and resolved issues in Junos Space Network Management Platform Release 23.1R1 hot patches.

During hot patch installation, the script performs the following operations:

- Blocks the device communication.
- Stops JBoss, JBoss-dc, and watchdog services.
- Backs up existing configuration files and Enterprise Application Archive (EAR) files.
- Updates the Red Hat Package Manager (RPM) files.
- Restarts the watchdog process, which restarts JBoss and JBoss-dc services.
- Unblocks device communication after restarting the watchdog process for device load balancing.

Installation Instructions

Perform the following steps in the CLI of the JBoss-VIP node only:

1. Download the Junos Space Platform 23.1R1 Patch VX from the Download Site.

   Here, X is the hot patch version. For example, V1, V2, and so on.

2. Copy the Space-23.1R1-Hotpatch-VX.tgz file to the /home/admin location of the VIP node.

3. Verify the checksum of the hot patch for data integrity:

   md5sum Space-23.1R1-Hotpatch-VX.tgz.

4. Extract the Space-23.1R1-Hotpatch-VX.tgz file:

   tar -zxvf Space-23.1R1-hotpatch-VX.tgz

5. Change the directory to Space-23.1R1-Hotpatch-VX.

   cd Space-23.1R1-Hotpatch-VX

6. . Execute the patchme.sh script from the Space-23.1R1-Hotpatch-VX folder:

   sh patchme.sh

   The script detects whether the deployment is a standalone deployment or a cluster deployment and installs the patch accordingly.

A marker file, /etc/.Space-23.1R1-Hotpatch-VX, is created with the list of RPM details in the hot patch.

NOTE:

- We recommend that you install the latest available hot-patch version, which is the cumulative patch.
- Set the SSH option “ServerAliveInterval” to a minimum value of 300, when connecting to the Applogic VIP through SSH to apply the hotpatch.

  Sample command: ssh admin@x.x.x.x -o ServerAliveInterval=300.

- When you configure the Disaster Recovery (DR), make sure that you reset the DR configuration on both the active and the standby sites.

Once the DR reset is complete, you must remove the **user.properties** file from the **/var/cache/jmp-geo/config** path for all the JBoss, database, and Fault Monitoring and Performance Monitoring (FMPM) nodes, if any.

New and Enhanced Features in the Hot Patch

Junos Space® Network Management Platform Release 23.1R1 hotpatch includes the following enhancements:

- Support for SRX1600 Firewall—Starting in Junos Space Network Management Platform Release 23.1R1 hot patch V2, we've provided support for SRX1600 firewall.
- Support for SRX2300 Firewall—Starting in Junos Space Network Management Platform Release 23.1R1 hot patch V2, we've provided support for SRX2300 firewall.

Supported Devices in the Hot Patch

Table 2 on page 24 lists the devices supported in Junos Space Network Management Platform 23.1R1 Hot Patch Releases.

Table 2: Supported Devices in the Hot Patch

Supported Device	Hot Patch Release Version
SRX1600	Junos Space Network Management Platform Release 23.1R1 Hot Patch V2
SRX2300	Junos Space Network Management Platform Release 23.1R1 Hot Patch V2

Resolved Issues

Table 3 on page 25 lists the resolved issues in Junos Space Network Management Platform Release 23.1R1 hot patch.

Table 3: Resolved Issues in Junos Space Network Management Platform Release 23.1R1 Hot Patch

PR	Description	Hot Patch Version
PR1867898	Junos Space fails to send E-mail notification when TLS is enabled.	v7
PR1880309	Execution of cleanUpJobs.sh results in the deletion of scheduled jobs.	v7
PR1861745	EX4300-48MP switches experienced Out-Of-Sync after the installation of patch 23.1R1HPV3.	v7
PR1860367	Junos Space Network Management Platform sends authentication requests to TACAS for a local user.	v6
PR1851757	The user is unable to upgrade the Junos firmware image from 23.4R2.13 to 23.4R2-S2.1 in the primary node of an SRX chassis cluster. The upgrade fails with an error.	v5
PR1773076	The user is unable to filter jobs from the job list.	v4
PR1787967	The Junos Space Network Management Platform GUI shows incorrect number of nodes under Network Monitoring.	v4

PR1811273	The user is unable to change Junos Space Network Management Platform GUI password when the original password contains special characters.	v4
PR1814883	When the user clicks the Save Filter option, Junos Space Network Management Platform GUI fails to respond.	v4

Table 3: Resolved Issues in Junos Space Network Management Platform Release 23.1R1 Hot Patch *(Continued)*

PR	Description	Hot Patch Version
PR1817241	While performing Test Connection in Junos Space Network Management Platform, it gets stuck with Testing.... Please wait... message.	v4
PR1818143	The model device configuration remains unaffected when a user adds an extra JBoss node to Junos Space Network Management Platform.	v4
PR1819315	The user is unable to add a new node in Junos Space Network Management Platform GUI.	v4
PR1828027	Multiple DMI sessions are not visible in Junos Space Network Management Platform GUI.	v4
PR1838157	The command jmp-dr toolkit watchdog status disable-automatic-failover duration 0 fails to disable the automatic failover permanently.	v4
PR1838492	SNMPD services stop on all Junos Space nodes after you perform jmp-dr manual failover.	v4
PR1842159	The management sessions in Junos Space Network Management Platform GUI are inconsistent and show incorrect data.	v4

Table 3: Resolved Issues in Junos Space Network Management Platform Release 23.1R1 Hot Patch *(Continued)*

PR	Description	Hot Patch Version
PR1846111	The Junos Space Network Management Platform GUI fails to collect logs as expected.	v4
PR1697264	Synchronization of Logical Systems (LSYS) for SRX Series Firewalls fails with the Exception is thrown during operationalRpcReq devId=### java.nio.channels.ClosedChannelException error message.	v3

PR1742243	Archive and purge job under Job Management fails with an error in Junos Space Network Management Platform Release 21.2R1.
	Workaround:
	1. In MySQL prompt, run the following command:
	`SET FOREIGN_KEY_CHECKS = 0;`
	2. Purge all the jobs carried out before 01.02.2023 from Junos Space Network Management Platform GUI.
	3. Return to MySQL prompt and run the following command:
	`SET FOREIGN_KEY_CHECKS = 1;`
		v3

PR1744314	Add More Device under Model Device takes longer than usual to open.	v3

Table 3: Resolved Issues in Junos Space Network Management Platform Release 23.1R1 Hot Patch *(Continued)*

PR	Description	Hot Patch Version
PR1754247	The Disaster Recovery page does not load in Junos Space Network Management Platform.	v3
PR1758864	The max_log_file_action is not set to ROTATE by default. Hence, the audit file logs are not purged and /var/log/audit is completely filled. Workaround: You can set the value for max_log_file_action in **/etc/audit/auditd.conf** file as ROTATE or KEEP_LOGS as per your requirement.	v3
PR1759990	Archive and purge jobs do not delete the following tasks: • Uninstall Application, and, • ICEAAA Manager clean up historic entries	v3
PR1765032	Junos Space Network Management Platform goes into maintenance mode frequently and displays Junos space is starting up, please wait message.	v3
PR1769758	Disaster recovery fails to synchronize sites.	v3
PR1770973	After Disaster Recovery failover, the jmp-dr health command intermittently shows jboss-dc: chkconfig(off!!) FAIL message.	v3

Table 3: Resolved Issues in Junos Space Network Management Platform Release 23.1R1 Hot Patch *(Continued)*

PR	Description	Hot Patch Version
PR1771233	Junos Space Network Management Platform GUI becomes unresponsive unless restarted.	v3
PR1771300	When you try to assign a template to a device in Junos Space Network Management Platform, it fails with Failed to release the lock on the device error message.	v3
PR1778019	Large fileHandleLeak.log is caused by large number of python processes.	v3
PR1779392	After jmp-dr starts, there is high network traffic on both active and standby sites and database logs display 1062 error repetitively.	v3
PR1781356	Multiple jobs are stuck in in-progress state.	v3
PR1782835	The Disaster Recovery manual failover test fails with fatal error 1236.	v3
PR1785850	After upgrading to Junos Space Network Management Platform Release 22.2R1 hot patch v3, when user cancels the Modify Template window without any changes, the Last Modified By name changes to the current user and the Last Update Time changes to the current time. Templates created on older versions also increment the latest version number.	v3

Table 3: Resolved Issues in Junos Space Network Management Platform Release 23.1R1 Hot Patch *(Continued)*

PR	Description	Hot Patch Version
PR1787517	When the user sets Out of Sync filter for Managed Status in the Device Inventory Report the system fails to generate any result. Workaround: Export all the values for Managed Status to CSV, and then set the Out of Sync filter.	v3
PR1788172	Archive and purge jobs fail with An error occurred while purging the information from JobInstance and its reference tables error.	v3
PR1659947	Junos Space Network Management Platform GUI shows incorrect number of nodes under Network Monitoring.	v1
PR1678536	Junos Space Network Management Platform shows incorrect timestamp in View Configuration Change Log under Device Management.	v1
PR1713174	The script @EXECUTIONTYPE = "GROUPEDEXECUTION fails to give the result when executed through API, images or script menu.	v1
PR1717146	Starting in Junos Space Network Management Platform Release 22.3R1, user fails to upgrade the ACX1100 and ACX2200 devices as the no-copy option is not available and the devices do not have sufficient space to hold copies of the software.	v1

Table 3: Resolved Issues in Junos Space Network Management Platform Release 23.1R1 Hot Patch *(Continued)*

PR	Description	Hot Patch Version
PR1731540	Users sees Fail in load selections data error while changing domains in the Device Management page and Job Management page.	v1
PR1732817	When you try to discover a device using the FIPS mode or SNMP, it fails with SNMPv3 AuthType should be SHA1 when the server is in FIPS mode error message.	v1
PR1734126	The database purging policy gets stuck in Junos Space Network Management Platform resulting in no data backup.	v1
PR1735659	Deleted devices continue to appear in the Network Monitoring node list even after deletion.	v1
PR1737025	The restart command on the Network Monitoring page, fails to restart the services.	v1
PR1738821	Resync Nodes job in OpenNMS page does not update the device progress in Junos Space Network Management Platform.	v1
PR1739065	Junos Space Platform Web GUI shows an error at times, when you upload PKCS12 format certificate.	v1
PR1740818	Resynchronization with the network fails with java.nio.channels.ClosedChannelException error.	v1

Table 3: Resolved Issues in Junos Space Network Management Platform Release 23.1R1 Hot Patch *(Continued)*

PR	Description	Hot Patch Version
PR1748467	After upgrading to Junos Space Network Management Platform 23.1R1, database status shows Out of Sync because of MySQL disk space utilization. Workaround: 1. Log in to Junos Space Network Management Platform CLI. 2. Edit the **/var/chroot/mysql/etc/my.cnf** file, to add: expire_log_days=3 3. Restart MySQL service using the following command: service mysqld restart	v1

Revision History

Release	Release Date	Updates
Junos Space Network Management Platform Release 23.1R1 Hot Patch V7	19 June, 2025—Revision 8	Added Resolved Issues
Junos Space Network Management Platform Release 23.1R1 Hot Patch V6	6 March, 2025—Revision 7	Added Resolved Issues

(Continued)

Release	Release Date	Updates
Junos Space Network Management Platform Release 23.1R1 Hot Patch V5	30 January, 2025—Revision 6	Added a Resolved Issue
Junos Space Network Management Platform Release 23.1R1 Hot Patch V4	3 December, 2024—Revision 5	Added Resolved Issues
Junos Space Network Management Platform Release 23.1R1 Hot Patch V3	6 August, 2024—Revision 4	Added Resolved Issues
Junos Space Network Management Platform Release 23.1R1 Hot Patch V2	27 December, 2023—Revision 3	Added the following in the Hot Patch: • New and Enhanced Features • Supported Devices
Junos Space Network Management Platform Release 23.1R1 Hot Patch V1	27 July, 2023—Revision 2	Added Resolved Issues
Junos Space Network Management Platform Release 23.1R1	8 June, 2023—Revision 1	Initial Release Notes