

Juniper Networks

Junos Space 2.0 Release Notes

November 15th, 2010
Revision 01 August 2011

Contents

Network Application Platform	2
New Features	2
Known Issues	4
Network Activate	5
New Features	5
Known Issues	6
QoS Design	6
New Features	6
Known Issues	7
Security Design	7
New Features	8
Known Issues	8
Resolved Issues	9
Service Insight	9
New Features	9
Service Now	10
New Features	10
Known Issues	10
Virtual Control	10
New Features	10
Feature Update	11
Operational Notes	11
Known Issues	11
Junos Compatibility	11
Troubleshooting Junos Space	13
Junos Space Technical Publications	13

Network Application Platform

The Junos Space Network Application Platform provides the essential tools the network administrator needs for automating network operations, including device discovery and management, topology visualization, deploying device images, job operation management, user account management, audit logging, and network administration. Network administration tasks include managing the Junos Space fabric (comprising one or more IP-connected nodes), database, licenses, applications, upgrades, tags, and troubleshooting.

New Features

The Junos Space Network Application Platform includes the following new features:

- **(Administration) Junos Space 2.0 Upgrade**—The Junos Space 2.0 software is bundled with Service Now and Service Insight. Junos Space 2.0 Hot-pluggable applications include:
 - Ethernet Design
 - Network Activate
 - QoS Design
 - Security Design
 - Virtual Control
- To upgrade to the Junos Space version 2.0 software from version 1.3 or 1.4, use the Platform > Administration > Manage Applications Upgrade Platform action.
- **(Scripts) Compare Script Versions**—Junos Space enables you to compare two scripts and view the differences in their content. You can compare two different scripts or two versions of the same script. Different colors are used to indicate differences between the compared scripts.
- **(Scripts) Automatic selection of the latest scripts**—Junos Space automatically picks the latest version of a script for deploying, verifying, enabling, disabling, and executing a script on devices. While the Manage Scripts page displays multiple versions of the same script, only the latest version of the script is picked even when you select an older version of the script.
- **(Devices) Support for WW Junos OS Devices**—The Junos Space wwadapter lets you use Junos Space to manage devices running the world wide version of Junos OS. These devices use Telnet protocol instead of Secure Shell protocol (SSHv2) for communication. The wwadapter acts as a medium between Junos Space and the device.
- **(Devices) Connecting to Device Discovery Target Using Telnet**—Junos Space connects to devices running worldwide Junos OS with the Connect via Telnet option on the Discover Target page.
- **[Release Candidate Test Quality] (Device Templates) Device Templates**—Device templates let you remotely deploy and update the JUNOS OS configuration running

on multiple devices on your network. Device template creation involves two major tasks:

- Creating and publishing a template definition based on configuration options for a Juniper Networks Junos OS device family DMI schema and device specific values.
- Creating, validating, and deploying a device template based on a template definition instance.

The network designer creates the template definition and assigns the network operator to deploy the template.

- **(Users) Create User-Defined Role**—Add one or more application workspace tasks per user-defined role using Platform > Users > Manage Roles > Create Role.
- **(Administration) Different Back Up Database Location**—The database back up location has changed from `var/lib/mysql/backup` to `/var/cache/jboss/backup`. To back up the Junos Space database, use Platform > Manage Databases > Backup Database.
- **(Administration) Configure New Application Settings**—Use the Platform > Administration > Manage Applications > Modify Application Settings action to configure the following setting. The look and feel of the Application Settings page has changed to a paged design instead of a dialog box.
 - *Allow users to auto log in to devices using SSH*—Allows users to automatically log in when starting an SSH connection on a device. The default, not selected, indicates that you have to add your credentials to log in to a device using SSH.
 - *Junos Space initiates connection to device*—Specifies connections between Junos Space and managed devices. If selected, Junos Space initiate connection with devices instead of the default behavior of device initiating connection.
 - *SSH port 22 for device connection*—Specifies the SSH port on the device. Junos Space uses this port to discover devices. The default value, 22, is the standard SSH server port.
- **(Administration Network Activate Application Settings**—Using the Platform > Administration > Manage Applications Modify Application Settings action, you can modify Network Activate application settings.
- **(Administration) Shutdown or Reboot a Fabric Node**—From Junos Space, the super administrator or system administrator can shut down or reboot fabric nodes (appliances or virtual machine hosts) when moved or network settings reconfigured. Use the Platform > Administration > Manage Fabric > Shut Down Node action. You can also type an optional message for administrators logged in to an affected node.
- **(Administration) Changing Node Network Settings**—Using Platform > Administration > Manage Fabric > Network Settings, you can change the following network settings:
 - VIP
 - Management IP, subnet mask and default gateway
 - Change, add or delete device management IP, subnet mask and default gateway

Nodes require restart to apply new network settings.

Known Issues

The following issues are known in Junos Space release 2.0:

- When you upgrade, the upgrade process generates an audit log. The upgrade audit log for an upgrade from 1.4 to 2.0 incorrectly indicates failure. We have identified that the root cause of this erroneous message is present in 1.4 code and produces the erroneous error message only in 1.4 to 2.0 upgrades. Please disregard the error and use alternative methods to verify success, such as viewing the platform version number. (PR 554026)
- If you modify the device management interface gateway from \ JMP_SETUP > -2(set routing), the Network Setting still display the old Value. It displays the correct IP value after you reboot the node. (PR 59885)
- Dynamic notification does not work for Service Now customers with Partner License. It works only for connected member in the Organization inventory page. (PR 526175)
- The Platform > Manage Applications upload process does not display an error message if it is interrupted. (PR 545034)
- The SSH connection state between Junos Space and a device still exists after automatic logout of the system occurs for an idle user. (PR 554372)
- On the Administration > Manage Fabric inventory page in tabular view, the cursor focus in the Console Message text box disappears and the text you are typing is not displayed if you type continuously in Console Message text box for approximately 20 seconds. Click in the Console Message text box to continue typing. (PR 551594)
- For a Junos Space initiated connection, the Platform > Manage Devices inventory page fails to switch to the new master Routing Engine on the dual Routing Engine on a JUNOS OS device. (PR 563648)
- Modifying a custom role sometimes does not show the task tree. Click Cancel, then modify the role again. (PR 564018)
- When you add a new node to a prime node fabric to which an upgraded version of WW Junos OS adapter has already been deployed, Junos Space does not automatically deploy the adapter to the new node. As a workaround, delete the adapter from the prime node before you add a new node to the fabric. After you add the new node, you can deploy the WW Junos OS adapter to both the nodes on the fabric. (PR 565798)]
- (Device Templates RCT Version) The template validation/deployment error messages are ambiguous and will be improved. (PR 564379)
- (Device Templates RCT Version) When you create a template definition, do not enter a lengthy description for a table or its label field. If the description occupies 3 or more lines of the Specify Default Values for Configuration Parameters page header, any message triggered by your input on that page would be below the visible part of the screen, for example the "Do you want to save this draft before you leave this page?" message that requires clicking a Yes or a No button. (PR 564751)
- (Device Templates RCT Version) Search results are under construction and will be improved. (PR 564769)

- (Device Templates RCT Version) When creating a template definition with an option of the 'choice' data type, be sure to complete all your settings on the tabs and click Next before you go on to another Configuration page in the Selected Configuration Layout panel. If you need to return to another page, click Back. (PR 565072)
- (Device Templates RCT Version) When you enter a term in the Search field, hitting Enter will not take you to the next occurrences of the term in the Available Configuration options list. (PR 565665)
- (Device Templates RCT Version) When creating a template definition and using the Search function, you cannot enter same search text sequentially (PR 565744)
- (Device Templates RCT Version) Do not leave the user interface idle for more than 19 minutes. (PR 564461)

Network Activate

Junos Space Network Activate software enables you to provision point-to-point and multipoint services across networks. You provision point-to-point services across networks that use LDP for signaling in the network core. These services use directed pseudowire virtual circuits across the network to establish point-to-point virtual private networks (VPNs). You provision multipoint services across networks that use BGP signaling in the network core. These VPLS services use route targets and route distinguishers to establish service connectivity. The Network Activate software supports multipoint-to-multipoint (full mesh) services and point-to-multipoint (hub and spoke) services.

New Features

The Network Activate application supports the following new features:

- **Aggregated Ethernet interfaces**—UNI interfaces for prestaged PE devices can be aggregated Ethernet (ae) interfaces.
- **Fast Ethernet interfaces**—UNI interfaces for prestaged PE devices can be Fast Ethernet (fe) interfaces. Fast Ethernet (fe) interface support is limited to specific Ethernet service configurations (on M Series devices with Junos 10.2R1.6). See “Prestaging Devices Overview” in the Network Activate user documentation for more information.
- **Force Deploying a Service**—When a service fails a configuration audit because configuration changes on a PE device do not match the configuration required for the service, you can force deploy the service to push the configuration to the device. Force Deployment pushes the same configuration to the device that was pushed during the deployment of the service, thus allowing the operator to recover from a state in which the configuration on the device was lost or changed out-of-band.
- **Multihomed groups**—Create one or more multihomed groups to connect a customer site to multiple N-PE routers to provide redundant connectivity across a VPLS site while preventing the formation of Layer 2 loops in the service provider's network. A VPLS site multihomed to two or more N-PE routers provides redundant connectivity in the event of a PE-router-to-CE-device link failure or the failure of an N-PE router.

- **QoS-enabled Ethernet services**—Attach a QoS profile to a point-to-point or multipoint (VPLS) service to define levels of service for UNI ingress and UNI egress traffic at the provider edge.
- **Services with flexible VLAN tagging**—Specify the asymmetric tag height Ethernet option to enable flexible VLAN tagging on VPLS services. A service with flexible VLAN tagging allows transport of Ethernet frames between UNI endpoints with mixed interface types (port, 802.1Q, and Q-in-Q). For example, a service normalized to 802.1Q that specifies port, 802.1Q, and Q-in-Q UNI endpoints performs the necessary pop, swap, or push operations to manipulate (inner and outer) VLAN tags to transport single-tagged frames across the UNI endpoints.
- **Enhancements to Normalization option**—Configure an Ethernet service with a specified interface type to transport frames with a different tag height. For example, you can create Layer 2 VPN Q-in-Q to Q-in-Q service that transports single-tagged frames or a Layer 2 VPN 802.1Q to 802.1Q service that transports double-tagged frames.

Known Issues

The Network Activate 2.0 release includes the following known issues:

- An AE interface that specifies one or more logical interfaces with assigned IP addresses is not a candidate for UNI role assignment. [562759]
- A Functional Audit might show incomplete information in the Functional Audit result window. [559092]
- Functional Audit might fail when you modify a service order by changing the role of an N-PE device in a multihomed group from primary to secondary and then deploy the service order, if the VPLS service definition specifies "Asymmetric_Vlan_Range_Normalize_to_vlan_all" with Advanced option, and auto-pick enabled. [565249]

QoS Design

The QoS Design application allows you to configure Quality of Service (QoS) features to provide improved service to certain network traffic on Ethernet services. Enabling QoS on an Ethernet service can improve network service by providing dedicated bandwidth, setting traffic priorities across the network, improving loss characteristics, shaping network traffic, and managing network congestion.

New Features

Create a QoS profile to configure classification and policing for UNI ingress traffic and policing, scheduling and shaping for UNI egress traffic on Ethernet services. The QoS Design application includes the following workspaces that allow you to define levels of service that you can then apply to Ethernet services in the Network Activate application:

- **QoS Domains**—Prestage QoS to partition your network into domains. A domain represents a group of N-PE routers for which the QoS treatment on the uplink interfaces is the same or similar. You can perform a single domain discovery operation to discover all the QoS domains on your network. Each QoS domain includes only those N-PE routers that share the exact rewrite rules and classifiers. If the scheduler maps are different, they are grouped in the domain as separate scheduler maps.
- **Drop Profiles**—Define parameters that allow packets to be dropped from the network. Drop profiles define the meanings of the loss priorities. When the number of packets queued is greater than the ability of the router to empty a queue, the queue requires a method for determining which packets to drop from the network.
- **QoS Schedulers**—A QoS scheduler defines the output queue properties for each class of service in the domain that is associated with the scheduler. Queue properties include the amount of interface bandwidth assigned to the queue, the size of the memory buffer allocated for storing packets, the priority of the queue, and the random early detection (RED) drop profiles associated with the queue. The QoS Design software supports two-level and three-level schedulers. A two-level scheduler is a shared scheduler (or scheduler profile) that allows logical interfaces belonging to the same physical port to share one set of scheduling properties. A two-level scheduler can also include a drop profile to reference WRED congestion control of the queue. With a three-level scheduler, scheduling is performed at the interface level and the scheduler defines two parameters—the port oversubscription ratio and the interface oversubscription ratio.
- **QoS Profiles**—A QoS profile is a configuration template that allows you to create service offerings that provide priority to certain traffic when you provision Layer 2 Ethernet Services. A QoS profile defines classification and policing for UNI ingress traffic and policing, scheduling, and rewrite rules for UNI egress traffic on the N-PE devices for Ethernet services.

Known Issues

The QoS Design 2.0 release includes the following known issues:

- Create scheduler issue when you deselect a class of service. If you clear the check box for some CoS rows and then edit one or more selected CoS rows, when you click **OK** the edited CoS rows that you configured are preserved. However, the CoS rows that were cleared before you clicked **OK** are automatically selected again. As a workaround, clear the checkbox for each CoS row that was automatically selected and then click **Create**. Only the CoS rows you intentionally selected are saved for the QoS scheduler. [565752]

Security Design

The Junos Space Security Design application is a powerful but easy-to-use solution that allows you to design a security topology that represents your physical network, create IPSec VPNs on different sections of your network to provide appropriate security on the network, and create security policies that define a set of rules to permit, deny or reject communication between security domains.

New Features

The Junos Space Security Design application presents the following new features:

- **CLI Preview for Provisioning IPSec VPNs and Security Policies**—The provisioning workflow for IPSec VPNs and security policies allows you to view the CLI format of the configuration pushed to the device.
- **Support for Screen OS Devices**— Screen OS devices are supported in IPsec VPN and Security Policy creation and deployment.
- **Policy VPN Integration**— When a security policy created between two security domains is provisioned, the policy will use the paths defined by the IPSec VPN created between the security devices associated with the security domains.
- **Security Policy for Intermediate Firewall**— An intermediate firewall with the security policy which allows IKE/IPsec traffic for VPN is configured automatically when provisioning a VPN with an intermediate firewall. The intermediate device is listed along with the VPN endpoints.
- **NAT**— Create, manage and provision NAT policies to devices. Using Network Address Translation (NAT), you can maintain network security by hiding internal IP addresses from other networks. You can also use NAT to conserve IP addresses. Junos Space supports two types of NAT:
 - **Source NAT**— Translates the source address of outbound traffic.
 - **Static NAT**— Maintains a constant one-to-one address translation. It translates the same private address to the same public address.

Known Issues

- If you create a device group with more than 100 devices, the device group will not be visible on the topology whiteboard.
Workaround: Click on the topology whiteboard. [PR 563375]
- When you decommission a VPN that has VPN Monitor setting enabled, VPN Monitor options such as Interval and Threshold are not removed from the device.
Workaround: Manually remove the VPN Monitor options using the CLI interface.
[PR 546065]
- If you create and configure a group link that has a large number of devices, the Link Properties window will still show that the group link is not configured. If you delete a group link that has a large number of devices, the link is still displayed on the topology whiteboard.
Workaround: Click on the topology whiteboard. [PR 561740]

Resolved Issues

- If you create two Provisioning Jobs to simultaneously provision two VPNs that use a common set of security devices, only the first Provisioning Job will succeed. The second Provisioning Job fails and displays an incorrect error message.

Workaround: You can either re-provision the second VPN that failed to provision after the first VPN's Provisioning Job is complete, or provision these VPNs, one at a time, ensuring that the first VPN's Provisioning Job is complete before you start provisioning the next one. [PR 544595]

Service Insight

The Junos Space Service Insight application accelerates operational analysis and manages exposure to known issues. The Junos Space Service Insight application presents the following new features:

New Features

The Junos Space Service Insight application presents the following new features:

- **Automated EOL analysis**—Identifying the devices available for End Of Life (EOL) reports and providing EOL information for those devices by enabling generation of EOL reports that provide detailed device EOL information, such as, the number of devices in the network with EOL parts, EOL announce date, number of EOL announce parts, End Of Engineering SW date, number of End Of Engineering SW parts, End Of Engineering HW date, number of End Of Engineering HW parts, End Of Support date, number of End Of Support parts, top level assembly parts, circuit assembly parts, PSN numbers, and replacement numbers. This helps ensure that software and devices are serviceable and you can upgrade and replace equipment that is no longer supported by Juniper Networks.
- **PBNs for preventive action**— Identifying devices with characteristics similar to devices on which issues were found and displaying Proactive Bug Notifications (PBNs) that provide information about issues, such as, the condition that triggered the issue, symptoms of the issue, temporary solutions to the issue, and additional instructions that users can follow to prevent the issue from occurring on the device. This is a proactive measure to ensure that users are aware of the known issues that could affect their network. Users can scan PBNs to display only those devices that are affected by a particular PBN, flag PBNs to users, assign owners to the PBNs, e-mail the PBNs to users, and delete them. Users can also list the PBNs that are associated to a particular device.
- **Notifications**— Notifying users about EOL and PBN information arrival and PBN information matches found for devices on the network. Managing these notifications and also creating filters that further specify when users must be notified, such as, the tag value that must match for the associated devices, the serial number or device name that must be matched, and the words that must or must not match the title of the PBN that has arrived. Users are allowed to edit notifications, enable or disable them, copy the attributes of notifications, and delete notifications.

Service Now

The Junos Space Service Now application streamlines fault management for JUNOS devices by automating the detection, isolation and resolution of network faults and incidents.

New Features

The Junos Space Service Now application presents the following new feature:

- **Installing AI-Scripts on Devices with Dual REs**—When you install AI-Scripts on devices with dual REs, Service Now installs AI-Scripts on both the primary and backup routing engines. After the AI-Scripts are installed, the Manage Jobs page and the Service Now Device Details dialog box display the status of installation for the individual REs (primary and backup).

Known Issues

- The connected members displayed on the **Manage Organizations** page will not receive dynamic notifications when Service Now operates in the partner proxy mode. [PR/526175]
- Junos OS devices may not provide specific time zones for incidents, and hence Service Now may display an incorrect time of occurrence for incidents. For example, when the time zone is EST, Service Now uses US EST by default, while the time zone can also be AEST (Australian EST). [PR/544087]
- The connection between the Service Now partner proxy and its end customers fails when a user changes the IP address of a Service Now partner proxy.

Workaround: Manually update the IP address of the Service Now partner proxy in your Service Now application. [PR/564827]

- Service Now cannot uninstall AI-Scripts from the back up RE of a device with dual REs. [PR/555657]

Virtual Control

New Features

This release of Junos Space Virtual Control presents the following new features:

- **Virtual Machine List**— View the list of virtual machines and their respective virtual NICs from the vNetwork workspace.
- **Block Virtual Ports**— Block and unblock virtual ports from Virtual Switch view.
- **Purging of Configuration Audit Results** — Purge configuration audit reports available from vNetwork view either by its age or count.
- **Cluster Support**— The JSVC will now work in a Cluster setup (JA Fabric setup).

Feature Update

- **Change in vNetwork Inventory view**— The vNetwork Inventory page has been changed from a tree view to table view in order to improve performance.

Operational Notes

- Junos Version 10.1R1 and above required for P+V orchestration support.
- JSVC has been qualified with EX4200 series of switches.
- JSVC has been qualified with VMware vSphere 4.0 and 4.1.
- Before starting P+V Orchestration, ensure that no other session (CLI/Web) is in Edit mode on the physical switches. Another session in edit mode will hold up the orchestration operation until the session is completed.

Known Issues

- Job Progress view for the Inventory Resync job does not display progress in actual terms. It displays the job at 0% until it is completed, and transitions it to 100% once it is completed. [PR 552950]
- Some of the GUI pages such as **Job Manager** may not refresh automatically. Please refresh the page manually to view the latest status. [PR 552955]
- Blocking (and unblocking) of virtual ports is allowed from JSVC even when the override policy is disabled in VMWare vCenter Server. [PR 552956]
- The special characters (/ , \ , %) in the virtual switches and port groups are not supported. Please avoid using these special characters while creating or modifying virtual switch and port group names.

Junos Compatibility

- Specific Junos OS releases and versions that fully support Junos Space 2.0 Platform are limited to the following:
 - Junos OS Release 9.3R4
 - Junos OS Release 9.4R3, R4
 - Junos OS Release 9.5R2, R3
 - Junos OS Release 9.6R1, R2, R3, R4
 - Junos OS Release 10.0R1, R2, R3, R4
 - Junos OS Release 10.1R1, R2, R3
 - Junos OS Release 10.2R1, R2, R3

- Junos OS Release 10.3R1
- Junos OS Release 10.4R1
- Specific Junos OS releases and versions that fully support Junos Space 2.0 Network Activate are limited to the following:
 - Junos OS Release 9.3R4
 - Junos OS Release 9.4R3, R4
 - Junos OS Release 9.5R2, R3
 - Junos OS Release 9.6R1, R2
 - Junos OS Release 10.0R1, R2
 - Junos OS Release 10.1R1
 - Junos OS Release 10.2R1
 - Junos OS Release 10.2R2
 - Junos OS Release 10.3R1
 - Junos OS Release 10.4R1
- Specific Junos releases and versions that fully support Junos Space 2.0 Service Now are limited to the following:
 - Junos Release 9.0 and later
- Specific Junos releases and versions that fully support Junos Space 2.0 Ethernet Design are limited to the following:
 - Junos OS Release 9.6R1, R2, R3, R4
 - Junos OS Release 10.0R1, R2, R3, R4
 - Junos OS Release 10.1R1, R2, R3
 - Junos OS Release 10.2R1, R2, R3
 - Junos OS Release 10.3R1
 - Junos OS Release 10.4R1
- Specific Junos OS releases and versions that fully support Junos Space 2.0 Security Design are limited to the following:
 - Junos OS Release 10.2R1, R2, R3
 - Junos OS Release 10.3R1
 - Junos OS Release 10.4R1

Troubleshooting Junos Space

For information about troubleshooting Junos Space, see:

http://www.juniper.net/techpubs/en_US/junos-space20/topics/concept/junos-space-troubleshoot-overview.html

Junos Space Technical Publications

Junos Space technical documentation is available as online help in the graphical user interface and on the Web in HTML and PDF file formats. The Web-based documentation is maintained after the final build of the online help, therefore use it wherever discrepancies exist between the help and the Web-based documentation.