

Junos Space 11.2 Release Notes

Contents

Network Application Platform	2
New Features	2
Operational Notes	3
Known Issues	4
Service Now	5
New Features	5
Operational Recommendation	5
Known Issues	6
Resolved Issues	6
Service Insight	6
New Features	7
Ethernet Design	7
New Features	7
Known Issues	7
Network Activate	7
New Features	8
Operational Notes	8
Known Issues	9
Transport Activate	9
Known Issues	10
QoS Design	10
New Features	10
Known Issues	11
Virtual Control	11
New Features	11
Operational Notes	12
Known Issues	12
Resolved Issues	13
Fault Management	13
Operational Notes	14
Known Issues	14
Hardware Support	15
Junos OS Compatibility	15
Troubleshooting Junos Space	16
Junos Space Technical Publications	16

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:

- **Junos Space 11.2 Upgrade**—The software is bundled with Service Now and Service Insight. Hot-pluggable applications include:
 - Ethernet Design
 - Network Activate
 - QoS Design
 - Virtual Control
- **Remote Authentication**—You can now maintain user authentication from a central location on one or more RADIUS servers using PAP and CHAP authentication methods. Junos Space, by default, authenticates users to log in locally when you configure their accounts from Platform > Users > Manage Users Create User. Now, from Platform > Administration > Manage Auth Servers you can allow users to log in from remote accounts or both remotely and locally and configure and test connection to remote authentication servers. Users stored on a RADIUS server contain no Junos Space role or authorization information, therefore you must configure it using Platform > Users > Manage Roles > Create Role , therefore you must create authorization for each user in Junos Space. Junos Space will not allow access if no user authorization exists locally.
- **Edit Device Configuration**—You can now edit the configuration files of any device managed by Junos Space. This easy-to-use editor has an interface that enables you not only to orient yourself in the configuration hierarchy without difficulty but also to access all configuration options in the DMI schema applied. It enables you to preview your changes and validate them before deployment. The validation message explains exactly what effect your changes will have on the device configuration.
- **Device Configuration File Management**—You can now manage device configuration files directly from a new workspace. The Manage Config File Actions include:
 - Backup (with versioning) of the configuration files of previously discovered devices;
 - View stored configuration files to display file name, creation time, version and file contents;
 - Compare two versions of one configuration file or any versions of two files;

- Edit configuration files, displaying entire file contents in the original format, and maintaining original pagination. New versions can be commented. The absence of a validation scheme or sanity check allows the advanced user complete freedom.
- Restore enables you to restore specified versions of selected configuration files to their respective devices, choosing between the Merge and the Override types of restoration.
- Export enables you to save specified versions of one or more configuration files to a zip file on your local computer.
- DMI Schema Management—All Juniper devices are configured via device management interface (DMI) schemas. Junos Space itself is based on the DMI interface. When new device features are developed, the device needs a new version of the schema to access those new features. DMI schema management enables you to bring any and all Juniper device schema versions under Space management and use them in applications such as Templates and Configuration Editor. No system restart is required. In Space -11.2 there are two ways to upload a DMI schema to Junos Space and update its repository:
 - By creating your own tgz file,
 - By checking out a DMI schema from the Juniper SVN repository.



NOTE: Importing a DMI schema from a device is not supported.

- Script Bundles—Group multiple scripts into a script bundle to deploy and execute the script bundle on Junos OS devices. You can also modify script bundles.

Operational Notes

- The upgrade package for Security Design was not released in 11.2. After you upgrade Junos Space to 11.2, Security Design will be grayed out.
- We recommend that you increase the login timeout value to **Never** or the maximum allowed (**120 minutes**) for the following operations:
 1. In Junos Space 2.0 and 11.1, before you upgrade to Junos Space 11.2, this action ensures that the UI session remains active during the upgrade process.
 2. When Junos Space manages a large network and you change device IP settings, this action ensures that the UI session remains active and the IP changes are transmitted to all the devices that Junos Space manages.
- For multi-node Space fabric upgrade to version 11.2 from versions 2.0 or 11.1: after finishing the upgrade and login, make sure all previously installed non-platform application icons show up as disabled before proceeding.

Known Issues

The Network Application Platform 11.2 release includes the following known issues:

- On the Schema Update page, the correct URL for the SVN repository is <https://xml.juniper.net/dmi/repository/trunk>. When entering this URL, do not include any leading or trailing spaces, as they are not correctly parsed. [PR-773679]
- When you launch resync jobs on a large number of devices simultaneously, paging in the Manage Devices inventory page may not function properly [PR 586001]
- Device reboot may trigger additional resyncs in Junos Space initiated connection scenarios, because Junos Space receives syslogs similar to FPC/PIC insertion, thus triggering resyncs. [PR 595664]
- In Configuration Editor, in certain cases the configuration options on the left hierarchy navigation pane do not match the content in the right pane. [PR 610782]
- When you delete a load balancer node from the fabric, a busy indicator appears. As a workaround, manually refresh your Web browser. [PR 579347]
- 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]
- Image Management: sometimes upload of large device images fails. The workaround is to retry the upload. [PR 579915]
- After you export a template, you find that configuration options whose data type is choice have changed names. [PR 580533]
- Device Templates: If you modify a template definition that is already being used in a template, that template might not be updated with the changes from the definition. As a workaround, create a new template based on the modified template definition. [PR 582435]
- In multi-node Space fabric, modifying user information from the Manage Users page will not trigger re-authentication users connected to other nodes. [PR 658923]
- In Configuration Editor, modify table key names and list values keeps the existing entry while adding a new entry with modified value [PR 662764]
- Modifying user information from the Manage Users page will trigger re-authentication for all users even though password information is not being modified. This may cause 'Authentication Failure' for the current session and re-login is required if there is password match failure with respect to current authorization mode settings. [PR 613237]
- When selecting the script bundle for image deployment in the Device Image deployment workflow, all script bundle names that are longer than 20 characters will display only 20 characters in the drop-down list. When modifying the script bundle in the Modify

Script Bundle workflow, only 20 characters are shown in the script bundle name. [PR 663799]

- Junos Space continues to use Telnet to communicate with a WW Junos OS device even after you have installed a non-WW Junos OS (domestic) image on the device. Similarly, Junos Space continues to use SSH to communicate with a non-WW Junos OS device even after you have installed a WW Junos OS image on the device.

Workaround: Delete the device and rediscover it. [PR 662611]

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:

- **SN MIBS**— Download Service Now MIBs from the Service Now homepage to enable your SNMP servers to receive traps sent from Service Now. To receive traps you must specify the SNMP servers in Service Now and also enable Service Now Notifications.
- **Auto Submit Policy**—Create and manage Auto Submit Policies to enable automatic submission of events that occur on Juniper Networks devices to Juniper Support Services (JSS).
- **Grouping different types of devices (Service Now Partner Proxy)**— Group the devices that are directly connected to Service Now and devices from a connected member in a single device group. You can also create a device group for every connected member and associate the device group to Service Now organizations dedicated to individual connected members. This enables you to track and organize technical support cases for a single end customer using different organizations (site IDs).
- **iJMBs submission to JSS**— iJMBs are uploaded to JSS once a week for every Service Now device.

Operational Recommendation

- When you upgrade Service Now operating in end-customer or partner proxy mode, ensure that the Service Now partner proxy is of the same version as its end-customer Service Now applications or up to 2 versions higher than the versions of the end-customer Service Now applications that it connects to.
- Read the KB article, <http://kb.juniper.net/KB19155>, before installing AI scripts on devices.

Known Issues

- Service Now does not support JMB processing for dual Routing Engine virtual chassis devices. [PR 614683]
- The status of a technical support case is not updated when the case is associated to a site ID that is not present in Service Now. [PR 575240]
- Service Now does not receive device configuration information (JMBs) from devices running Junos OS 11.2, which have AI-Scripts Install-Package Release 2.1R1 to 2.6R2 installed.

Workaround: Use AI-Scripts Install-Package Release 2.6R2.1 or later. [PR 584236]

- 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]

Workaround: See

http://www.juniper.net/techpubs/en_US/junos5/information-products/topic-relationships/working-system-basis/time-zone-custom-config.html for information on how to configure a custom time zone.

- 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]
- The AI-Script Install package is not deleted from EX Series devices even if you select the 'Remove Script Bundle files after successful install' option during event profile installation in Service Now. [PR 662499]

Resolved Issues

- Service Now does not support JMB processing for MX80-48t devices.

Workaround: Use AI-Scripts install-package 2.6R2. [PR 578428]

Service Insight

The Junos Space Service Insight application accelerates operational analysis and manages exposure to known issues.

New Features

This release of the Junos Space Service Insight application does not introduce new features.

Ethernet Design

The Junos Space Ethernet Design application provides you with a workflow enabling you to simultaneously configure and manage multiple Junos devices within a network.

New Features

The Junos Space Ethernet Design application presents the following new feature:

- **Support for QFX3500 Switches**— Junos Space provides you with four additional port profiles that you can provision to Juniper Networks QFX3500 switches.
 - **Fibre Channel Port Profile**— Enables the port to connect to a storage area network (SAN) switch. You can apply this profile to Fibre Channel ports on QFX3500 switches that function as FCoE-FC gateway switches.
 - **FCoE Gateway Port Profile**— Enables the port to connect to FCoE devices. You can apply this profile to all 10-Gigabit Ethernet ports.
 - **Network FCoE Transit Port Profile**— Enables the QFX3500 switch to act as a Fibre Channel transit switch that connects a transit switch to the network. You can apply this profile to all 10-Gigabit Ethernet ports. The profile is enabled on interfaces that face the network.
 - **Server FCoE Transit Port Profile**— Enables the QFX3500 switch to act as a Fibre Channel transit switch that connects a transit switch to an FCoE server. You can apply this profile to all 10-Gigabit Ethernet ports. The profile is enabled on interfaces that face the server.
- **63 Port Configuration**— By connecting an optical splitter, you can convert each QSFP+ uplink port in a QFX3500 switch to a set of four 10-Gbps Ethernet ports (xe ports). Ethernet Design enables you to apply port profiles to these fifteen 10-Gigabit Ethernet ports (port 0 is reserved). This way, you can extend the number of ports available for configuration to 63 ports.

Known Issues

- Provisioned Native and VoIP VLANs are not listed in the **Port Configurations Parameters** dialog box when you try to reconfigure a port. These provisioned VLANs are also not displayed on the **View Port Associations** page. This issue occurs in VLAN-port associations created in Junos Space prior to the 11.1 Release. [PR 576159]

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. Network Activate software also enables you to provision Layer 3 VPN full mesh services.

New Features

The Network Activate 11.2 release includes the following new features:

- **One-interface Hub-and-Spoke BGP/Static or OSPF/Static Layer 3 VPN Predefined Service**—You can create a one-interface hub-and-spoke BGP/static or OSPF/static Layer 3 VPN service based on a predefined service definition. Create a service definition from Service Design > Manage Service Definitions > Create L3VPN Service Definitions. Create a service order from Service Provisioning > Manage Service Orders > Create L3VPN Service Order. In a one-interface hub-and-spoke topology, there is only one interface using a combination of static routes, BGP, and OSPF routes between CE hub and PE hub routers. Use a one-interface hub-and-spoke Layer 3 VPN service definition to configure a service to advertise a default route from a hub to the spokes.
- **IPv4 IP Address Management**—Instead of having to manually allocate IP addresses to configure Layer 3 VPNs, IP address management allows Network Activate to automatically assign consistent IPv4 IP addresses on both sides of each PE/CE link and keep track of which IP addresses are already in use. Network Activate provides two categories of IP address pools: global and customer. Global pools are one or more IP address pools for service provider; customer pools are one or more IP address pools for a particular customer. Create IP address pools at the beginning of Network Activate Prestaging, before Role Discovery so that any IP addresses are found on devices during role discovery. When IP addresses are used in the pool, you can not use them.

From Service Design > Manage Service Definitions > Create L3VPN Service Definition, you can specify an IP address pool during L3VPN service definition configuration to use when assigning IP addresses for each PE/CE link. From Service Provisioning > Manage Service Orders > Create L3VPN Service Order, Network Activate automatically assigns IP address pools for each PE/CE link, if allowed by the service definition.

- **Service Templates Enhancements**—The Service Templates Enhancements enable you to design a service with attributes not natively supported in Service Provisioning. In combination with the Flexible Service Attributes editor, use it to configure any future device functionality--as and when available--without upgrading Network Activate.

Operational Notes

- Upgrading from Junos Space 2.0 to 11.2: if you already have QoS Design in Junos Space 2.0, upgrade QoS Design first, before you upgrade Network Activate. You will notice that some icons on the QoS navigation ribbon are missing after upgrading Network Activate. Do a server restart from the Fabric Manager UI (using Shutdown Node option) and the icons will appear.
- During Service Template creation if you want to add typed-in text along with Service Specific variables, you must press **Enter** after you type in the text.

Network Activate 11.1 to 11.2 Upgrade

- The two Layer 3 VPN standard (full-mesh) service definitions installed by Network Activate 11.1, L3VPN-BGP-Static and L3VPN-OSPF-Static, are marked as DEPRECATED. In the deprecated state, you can view them using the Manage Service Definitions inventory page. You can view the IPv4 attribute labels on the Service Definition Details page. You can not publish or unpublish these two deprecated Network Activate 11.1 service definitions, therefore they are not available for use in new Network Activate 11.2 service orders. These two service definitions do not appear in the list of selectable service definitions when you create a new Network Activate 11.2 Layer 3 VPN service order.
- Four new Network Activate 11.2 Layer 3 VPN standard (full-mesh and hub-and-spoke) service definitions are installed by the Network Activate 11.2 upgrade, all four of which include Network Activate 11.1 IPv4 attributes. In the upgrade case, these service definition names end in **-IPv4Mgt** to distinguish them from the Network Activate 11.1 service definition names.
- When you perform a fresh install starting right from Network Activate 11.2, the four standard Layer 3 VPN service definition names do not end in **-IPv4Mgt**.
- You can not modify any upgraded Network Activate 11.1 service instances that were derived from Network Activate 11.1 service definitions. You can not add new Layer 3 UNIs to 11.1 service instances. Attempting to save a modification to the database or deploying the modification fails when the server-side validation fails to find any customer IPv4 pool containing each of the IPv4 IP addresses that were manually assigned back in Network Activate 11.1.
- You can decommission Network Activate 11.1 service instances derived from 11.1 service definitions. This is the workaround from upgrading the 11.1 services: Decommission the old 11.1 services and recreate them by creating new (equivalent) 11.2 Layer 3 VPN services using 11.2 standard or custom service definitions.
- It is not possible to create new Network Activate 11.2 Layer 3 VPNs using the two 11.1 service definitions, since they have been put in the DEPRECATED state. You can only create new 11.2 Layer 3 VPNs using the published 11.2 service definitions (with IPv4 attributes), or new 11.2 custom service definitions (with IPv4 attributes).

Known Issues

The Network Activate 11.2 release includes the following known issues:

- Service Templates—Modifying a service to delete a PE device and add a new one does not remove the template configuration for the old PE device. [PR 612101]
- L3VPN deployment on FE interfaces with Ethernet option as VLAN is not supported. Only the FE Ethernet port option is supported now. [PR 582460]

Transport Activate

Transport Activate allows you to design, provision, and deploy MPLS-dynamic and RSVP-signaled label-switched path (LSP) services that run from a specific ingress router

to a specific egress router. You can configure end-to-end point-to-point and point-to-multiple-point LSPs.

Transport Activate is integrated with and codependent upon Network Activate, that provides Layer 2 and Layer 3 VPN service provisioning. Therefore, to use Transport Activate, you must install Network Activate first.

Provisioning an LSP service includes the following major tasks:

- Discover Juniper Networks devices that have been configured for MPLS-Signaled LSP into Junos Space using the Devices workspace. See the MPLS-Signaled LSP Configuration Guidelines in the *Junos OS MPLS Applications Configuration Guide*.
- Discover LSP devices from the Junos Space Platform database using **LSP Provisioning > Manage LSP Devices > Discover LSP Devices**.
- Assign LSP roles to provide authorization for the LSP definition designer and service activator to provision LSP services using Junos Space **Platform > Users**.
- Create an LSP definition to use to create an LSP service using **LSP Design > Manage LSP Definitions > Create LSP Definition**. You can configure LSP settings in the LSP definition so that they are configurable in the LSP service order.
- Create and validate LSP services using **LSP Provisioning > Manage LSPs**.

Known Issues

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.

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 lets you to define levels of service that you can then apply to Ethernet services in the Network Activate application:

New Features

The QoS Design application includes no new features in this release.

Known Issues

- There is a 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 check box 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. [PR 565752]

Virtual Control

New Features

Virtual Control includes the following new features:

- **vSwitch Life Cycle Management**—JSVC now provides an option to manage the entire life cycle of a virtual switch. This includes creation, modification and deletion of vSwitches.
- **vSwitch Profile Management**—JSVC provides an option to create profiles that can be applied on vSwitches. A vSwitch profile encapsulates the hardware independent configuration of a virtual switch that can be shared across virtual switches. vSwitch profiles facilitate one-touch provisioning of same port groups seamlessly across virtual switches spanning different hosts.
- **Detailed status of an Orchestration Job**—JSVC now provides additional details for an orchestration job. It includes the details on the configuration being orchestrated (from vSwitches & port groups) and on to which physical ports associated to physical NICs of hosts is specified.
- **VMKernel and Service Console Port Groups Life Cycle Management**—JSVC now supports the configuration of a management network for a Host/Hypervisor. It involves the lifecycle management of VMKernel and Service Console connection types.
- **Viewing Associated Entities (Filtered View)**—JSVC now provides an option to view the associated entities on their respective landing pages through a filtered view. For example, from the hosts ILP, the user can view the vSwitches that are associated to a particular host; the Manage vSwitches page will be filtered by the associated host and shown.
- **Viewing Host and VM associations from a DVS**—JSVC now provides options to view the associated Hosts and associated VMs from a Manage vSwitches page. Unlike the other filtered views, this view will provide details on the connectivity related parameters like NIC, NIC Type, Port Group etc. These views are invoked by right clicking on a distributed vSwitch and selecting “View Host Association” or “View VM Association” menu.
- **Datacenter support**— A new hierarchy called “Datacenter” is introduced in JSVC under a vNetwork to logically group the entities and keep them inline with the VMWare

vCenter. The entities like vSwitch and Hosts will now be shown with the datacenters under which they belong to.

- **Optimization of Port Group Profiles**—JSVC now handles the Port Group profiles management in an optimized way by avoiding duplicate discovered profiles with same configuration.
- **Display of Additional Information for entities**—JSVC now displays second level description in the landing pages of all entities (Hosts, VMs, vSwitches, Port Groups etc) to provide the user with additional details about the entity.
- **Viewing Detail Summary for Managed entities**—JSVC now displays the Summary window with details of an entity when it is double clicked or “Details” link is clicked on the image view from their respective ILPs.

Operational Notes

- Junos Version 10.1R1 and above required for P+V orchestration support.
- Junos version 10.4R1 and above is required for Private VLAN orchestration support.
- JSVC has been qualified with EX4200 and EX 4500 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

- After upgrading from JSVC 2.0 or 11.1 to JSVC 11.2, the association between the physical NICs of the host and the physical switch ports will be removed. Therefore, it is recommended that you make a note of all the associations, and re-associate them manually (or through a CSV file import) after upgrading to JSVC 11.2. [PR 661794]
- While upgrading from older version (from 2.0 to 11.2 or 11.1 to 11.2) to the current version of JSVC, It is required that the VMWare vCenter server is connected and reachable from JSVC. Else the vCenters that are not reachable will be removed from the JSVC database. It is also recommended that user does not perform any operations on the VMWare vCenter during the upgrade process. [PR 662506]
- The standalone vSwitch port group association to virtual machine made on VMWare vCenter may not reflect in JSVC immediately due to the limitation with VMWare APIs. The changes will reflect after a manual (or the periodic) re-synchronization is completed. [PR 661783]
- Renaming a standalone vSwitch port group from VMWare vSphere client creates a new port group profile and associates it to the port group in JSVC. This is due to the limitation of VMWare APIs hence it is recommended to modify any standalone vSwitch port group from JSVC instead of vSphere client. [PR 661787]
- The MAC address of a virtual machine that is associated to a VSS port group may not be properly reflected in the Virtual Control. This is due to the limitation of VMWare

APIs. Alternatively, user can refer the VMWare vCenter for MAC address details. [PR 661777]

- IP address of a virtual machine may not be reflected in Virtual Control dynamically if the IP address is assigned by a DHCP server in the VMWare vCenter. This is due to the limitation of VMWare event notifications. The IP address will reflect after a manual (or periodic) re-synchronization is completed. [PR 661790]
- While modifying a vSwitch, the “vSwitch General Settings” page may not be loaded completely and the user may not be able to select any values from the fields. In this situation, canceling and reopening of the screen will solve the issue. [PR 661806]
- DVS - Host association is shown in JSVC albeit this association is removed while moving a disconnected Host from one Datacenter to another in the VMWare vCenter side. It will be automatically deleted by JSVC during the next synchronization cycle (or) at the time of processing a DVS / Host related event notification. [PR 662292]
- JSVC allows deleting a DVS which has association with kernel or consoling NIC whereas VMWare vCenter does not. If user tries this operation from JSVC it will fail in vCenter and the object will be in “Delete requested” state in JSVC. Manual re-synchronization is required if user wants to perform any operation on that DVS immediately. Otherwise this state will be automatically changed to insync during the next synchronization cycle or at the time of processing a DVS related event notification. [PR 662900]

Resolved Issues

- The Job Progress view does not indicate the progress accurately for some jobs, when they are running. It displays the job progress at 0% until the job is completed and then transitions to 100%, once the job is completed. This has been fixed for orchestration and discovery.
- Blocking (and unblocking) of virtual ports is allowed from JSVC even if the override policy is disabled in vCenter. This has been fixed and now blocking and unblocking will not be allowed from JSVC if the override policy is disabled in vCenter. [PR 552956]

Fault Management

Junos Space Fault Management lets you discover Juniper Networks devices, then view and manage alerts and events in realtime to proactively manage network operation and performance.

Fault Management is an integration with IBM® Tivoli® Netcool® OMNIbus and IBM Tivoli Netcool Manager (ITNM) with Juniper Networks Junos Space, version 11.2. The Fault Management documentation provided is not rebranded and is developed by IBM Corporation.

Fault Management supports the following features:

- **Administration > Event Management Tools**—Filters, views, tool creation, menu configuration, maps, CGI registry, event database query, and maps
- **Administration > Network**—Network polling and path view administration

- **Availability > Network Availability**—Network Health View, Fault-Finding View, Network Views, Network Hop View, Path Views, SNMP Web Browser, SNMP MIB Graph, Event Dashboard
- **Availability > Events**—Event Dashboard, performance graphs, Active Event List (AEL), table view, Lightweight Event List (LEL), table view, geographic maps, and e-commerce maps
- **Discovery**—Network discovery status and configuration

From Fault Management, you can switch to other Junos Space applications using the Application Switcher global button in the upper right corner of the page.

You can open the Fault Management AEL (Active Event List) page using the Platform > Devices > Manage Devices > View Faults . The list is filtered by the selected IP addresses.

Operational Notes

Fault Management has the following operational notes:

- Fault Management does not support Firefox 4.0.
- Upload the Fault Management image using the SCP option; not the HTTP upload.
- If installing Fault Management on a virtual appliance, free disk space should be greater than 40GB
- On a multi node fabric failover is not supported for Fault Management application, if a node running Fault Management application goes down, it does not get started on the other node.
- In case of multi node fabric installed with Fault Management application, all the data related to this application will be stored only on the node running the application, If that node is deleted, the application gets started on the other node, but existing data is lost.

Known Issues

Fault Management includes the following known issues:

- Fault management's **Add Application** job takes approximately one hour to complete per node. On a single node fabric setup, it therefore takes one hour. On a multi-node fabric, the installation is serial, so on a two-node setup it takes approximately two hours. [PR 658912]
- Fault Management is not installed on the new nodes added to the fabric. [PR 658927]
- In a multiple-node (greater than two) Junos Space deployment, Fault Management is enabled in first database node. All other nodes have Fault Management installed, but not running. It gets started on the other database node only when you delete the existing node running the Fault Management application. [PR 658918]
- **Junos Space server is starting** message appears when you uninstall Fault Management application. Restart the HTTPD service to get the Junos Space user interface. [PR 613189]

Hardware Support

The Junos Space software supports all platforms in the following product series. For the latest platform support, see the Junos Space Platform and application data sheets.

- MX Series devices
- M Series devices
- T Series devices
- J Series devices
- EX Series devices
- SRX devices
- QFX devices
- BX devices

Junos OS Compatibility

- Specific Junos OS releases and versions that fully support Junos Space 11.2 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
 - Junos OS Release 11.1R1
 - Junos OS Release 11.2R1
- Specific Junos OS releases and versions that fully support Junos Space 11.2 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
- Junos OS Release 11.1R1
- Junos OS Release 11.2R1
- Specific Junos releases and versions that fully support Junos Space 11.2 Service Now are limited to the following:
 - Junos Release 9.0 and later
- Specific Junos releases and versions that fully support Junos Space 11.2 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
 - Junos OS Release 11.1R1
 - Junos OS Release 11.2R1

Troubleshooting Junos Space

For information about troubleshooting Junos Space, see:

http://www.juniper.net/techpubs/en_US/junos-space11.1/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.