

Junos Space Virtual Appliance Installation and Configuration Guide

Published
2020-11-04

Release
19.3

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

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

Junos Space Virtual Appliance Installation and Configuration Guide
19.3

Copyright © 2020 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation | vi

Documentation and Release Notes | vi

Documentation Conventions | vi

Documentation Feedback | ix

Requesting Technical Support | ix

Self-Help Online Tools and Resources | x

Creating a Service Request with JTAC | x

1

Virtual Appliance Overview

Junos Space Virtual Appliance Overview | 12

Configuring an NTP Time Source for Each Appliance Overview | 12

Ethernet Interfaces in a Junos Space Virtual Appliance Overview | 13

2

Deploying the Junos Space Virtual Appliance

Junos Space Virtual Appliance Deployment Overview | 19

Deploying a Junos Space Virtual Appliance on a VMware ESXi Server | 23

Installing the VMware ESXi Server | 24

Installing a Junos Space Virtual Appliance on a VMware ESXi Server | 25

Installing a Junos Space Virtual Appliance by Using vSphere Client | 25

Installing a Junos Space Virtual Appliance by Using the OVF Tool | 26

Modifying RAM Settings for a Junos Space Virtual Appliance | 27

Adding Disk Resources for a Junos Space Virtual Appliance | 28

Deploying a Junos Space Virtual Appliance on a KVM Server | 28

Installing a Junos Space Virtual Appliance on the KVM Server by Using VMM | 29

Modifying the Type of Virtual Disk Interface | 31

Modifying RAM for a Junos Space Virtual Appliance | 32

Adding Disk Resources for a Junos Space Virtual Appliance | 32

Enabling Multicast on Bridged Interfaces of a KVM-Host Machine | 32

Adding Disk Resources for a Junos Space Virtual Appliance | 33

Adding Disk Resources for a Junos Space Virtual Appliance Deployed on a VMware ESX or VMware ESXi Server | 35

Adding Disk Resources for a Junos Space Virtual Appliance Deployed on a KVM Server | 36

Starting Open VM Tools in Junos Space Platform | 37

Installing VI Toolkit for Perl on Junos Space Virtual Appliance | 39

Configuring the Junos Space Virtual Appliance

Configuring a Junos Space Virtual Appliance as a Junos Space Node | 43

Configuring a Junos Space Virtual Appliance | 45

Configuring Access to Junos Space Through a NAT Gateway | 62

Configuring the eth1 Ethernet Interface | 68

Configuring a Junos Space Virtual Appliance as a Standalone or Primary FMPM Node | 70

Configuring the Junos Space Virtual Appliance as the Primary FMPM Node | 71

Configuring a Junos Space Virtual Appliance as a Backup or Secondary FMPM Node for High Availability | 81

Configuring a Junos Space Virtual Appliance as a Backup or Secondary FMPM Node | 83

Changing the Network and System Settings of a Junos Space Virtual Appliance | 89

Changing the admin User Password of a Junos Space Virtual Appliance | 90

Changing the Network Settings of a Junos Space Virtual Appliance | 92

Adding a DNS Server | 93

Deleting a DNS Server | 95

Modifying the Virtual IP Address | 96

Modifying the IP Address of the eth0 Interface | 100

Modifying the NAT Configuration | 106

Modifying the IP Address of the eth1 Interface | 111

Modifying the IP Address of the eth3 Interface | 113

Adding Static Routes to a Junos Space Virtual Appliance | 119

- Deleting Static Routes from a Junos Space Virtual Appliance | 124
- Changing Time Options of a Junos Space Virtual Appliance | 126
 - Changing the Time Zone | 126
 - Changing NTP Settings | 128
- Retrieving System Log Files from a Junos Space Virtual Appliance | 130
- Expanding the Drive Size of a Junos Space Virtual Appliance | 132
- Setting Security Options on a Junos Space Virtual Appliance | 135
 - Enabling the Firewall on a Junos Space Virtual Appliance | 135
 - Disabling the Firewall on a Junos Space Virtual Appliance | 136
 - Disabling SSH on a Junos Space Virtual Appliance | 136
 - Enabling SSH on a Junos Space Virtual Appliance | 137
- Running Shell in a Junos Space Virtual Appliance | 138

4

Viewing and Adding Nodes to a Fabric

Adding a Node to an Existing Junos Space Fabric | 141

- Adding a Junos Space Node to the Junos Space Fabric | 142
- Adding an FMPM Node to the Junos Space Fabric | 147
- Obtaining Fingerprint of a Junos Space Node | 149

Viewing Nodes in the Fabric | 150

- Changing Views | 151
- Viewing Fabric Node Details | 151

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | vi
- Documentation Conventions | vi
- Documentation Feedback | ix
- Requesting Technical Support | ix

Use this guide to install and configure the Junos Space Virtual Appliance. After completing the installation and basic configuration procedures covered in this guide, refer to the Junos Space Network Management Platform documentation for information about further software configuration.

Documentation and Release Notes

To obtain the most current version of all Juniper Networks[®] technical documentation, see the product documentation page on the Juniper Networks website at <https://www.juniper.net/documentation/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <https://www.juniper.net/books>.

Documentation Conventions

Table 1 on page vii defines notice icons used in this guide.

Table 1: Notice Icons







Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page vii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

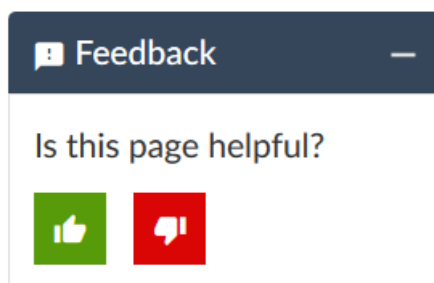
Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

1

CHAPTER

Virtual Appliance Overview

[Junos Space Virtual Appliance Overview | 12](#)

[Ethernet Interfaces in a Junos Space Virtual Appliance Overview | 13](#)

Junos Space Virtual Appliance Overview

The Junos Space Virtual Appliance consists of preconfigured Junos Space Network Management Platform software with a built-in operating system and application stack that is easy to deploy, manage, and maintain.

A Junos Space Virtual Appliance includes the same software and all the functionality available in a Junos Space physical appliance. However, you must deploy the virtual appliance on a VMware ESX, VMWare ESXi or KVM server, which provides a CPU, hard disk, RAM, and a network controller, but requires installation of an operating system and applications to become fully functional.

Just as you can install additional physical appliances to create a fabric to provide scalability and availability, you can deploy multiple virtual appliances to create a fabric that provides the same scalability and high availability as a fabric of physical appliances.

A Junos Space fabric can contain only physical appliances (JA2500), only virtual appliances, or a combination of both physical and virtual appliances.

Configuring an NTP Time Source for Each Appliance Overview

To ensure consistent behavior among all nodes in a multinode fabric, the time on each node must be synchronized with every other node in the fabric. When you configure the first Junos Space Virtual Appliance with a Network Time Protocol (NTP) server, you must ensure that, if the first node (which is used to synchronize time for all nodes in the fabric) goes down, all the other nodes in the fabric remain synchronized. Additional nodes installed in the same fabric automatically get their time setting from the first node in the fabric without any additional NTP server configuration.

NOTE: By default, Junos Space Network Management Platform synchronizes the local time zone of the client computer with the time zone of the server so that the Web user interface displays the Junos Space server time in the local time zone. However, the CLI server displays time as per the time zone configured on the Junos Space server.

To ensure that time remains synchronized across all nodes in a fabric, we strongly recommend that you add an NTP server to the first appliance (physical or virtual) during the initial setup.

NOTE: You must add the NTP server before you add the appliance or node to the fabric from the Junos Space user interface.

RELATED DOCUMENTATION

Junos Space Virtual Appliance Deployment Overview 19
Configuring a Junos Space Virtual Appliance as a Junos Space Node 43
Configuring a Junos Space Virtual Appliance as a Standalone or Primary FMPM Node 70
Adding a Node to an Existing Junos Space Fabric 141

Ethernet Interfaces in a Junos Space Virtual Appliance Overview

A Junos Space Virtual Appliance contains four Ethernet interfaces—eth0, eth1, eth2, and eth3. The Ethernet interfaces eth0 and eth3 support both IPv4 and IPv6 addresses. As a separate IP address is available for each IP stack, for any connection initiated by Junos Space, the source IP address (that is, the IPv4 or IPv6 address) of the connection is bound by the IP address type of a managed device. For a connection initiated by a managed device, Junos Space listens on both IPv4 and IPv6 addresses of the device management interface (eth3). Therefore, a managed device can communicate with Junos Space by using its IPv4 or IPv6 address.

NOTE: From Junos Space Network Management Platform Release 14.1R2 onward, you can configure Junos Space Ethernet interfaces with only IPv4 addresses, or both IPv4 and IPv6 addresses.

Junos Space supports managed devices based on the IP address type (that is, the IPv4 or IPv6 address) configured for the device management interface. You can configure an IPv4 or IPv6 address for the device management interface. If the device management interface is not configured, the IP address type of the node management interface (eth0) is considered for communication with managed devices. [Table 3 on page 14](#) details the support matrix for IPv4 and IPv6 address configurations on the device management interface.

Table 3: Matrix for IP Address Versions Supported on Devices

eth0		eth3		IP Address of Managed Devices Supported by Junos Space
IPv4 Address	IPv6 Address	IPv4 Address	IPv6 Address	
Configured	Not Configured	Not Configured	Not Configured	IPv4
Configured	Configured	Not Configured	Not Configured	IPv4 and IPv6
Configured	Not Configured	Configured	Not Configured	IPv4
Configured	Not Configured	Configured	Configured	IPv4 and IPv6
Configured	Not Configured	Not Configured	Configured	IPv6
Configured	Configured	Configured	Configured	IPv4 and IPv6

You can use the Ethernet interfaces of Junos Space as follows:

- **eth0**—Use the eth0 interface to configure the virtual IP (VIP) address of a fabric and the IP address of the node as well as to access the managed devices. The VIP address and the IP address of the node should be on the same subnet.

The eth0:0 subinterface provides access to the Junos Space Network Management Platform GUI. You can access the GUI by using the VIP address of the fabric.

- **eth1**—Use the eth1 interface as an administrative interface of a Junos Space node. Use SSH to access a Junos Space node through this interface. The eth0 interface and the eth1 interface can be on different subnets.

If you configure eth1, SSH stops running on the eth0 and the eth3 interfaces. You can access the CLI of the Junos Space virtual appliance only through the eth1 interface.

NOTE: From Junos Space Network Management Platform Release 14.1R1 onward, you can configure the eth1 Ethernet interface as an administrative interface.

- **eth2**—The eth2 interface is reserved for future use.
- **eth3**—Use the eth3 interface for SSH access to managed devices when the managed devices are on an out-of-band management subnet or on a subnet not accessible through the eth0 interface.

NOTE:

- If the managed devices are not accessible through the default gateway, you must configure static routes. Any static route configured manually is populated in the main routing table, which is used to route traffic through the eth0 interface.
- When the eth3 interface is configured as a device management interface, Junos Space Platform does not forward ICMP packets through the eth3 interface. To allow ICMP packets through the eth3 interface, routes must be added manually.

NOTE: When you configure a node as an FMPM node, you can use only the eth0 and eth1 interfaces.

- When you configure an appliance as a Junos Space node, you can configure the Ethernet interfaces as follows:

- Configure only the eth0 interface.

When only Ethernet interface (eth0) is used, the Junos Space nodes in the fabric, virtual IP (VIP) address of the fabric, and the devices being managed by Junos Space are on the same subnet.

- Configure the eth0 and eth3 interfaces.

When Ethernet interfaces eth0 and eth3 are used, the Junos Space nodes in the fabric and VIP address of the fabric are on the same subnet and are reachable through Ethernet interface eth0. The devices being managed by Junos Space are on the same subnet, which is different from the one reachable through Ethernet interface eth0, and are reachable through Ethernet interface eth3.

- Configure the eth0 and eth1 interfaces.

When Ethernet interfaces eth0 and eth1 are used, the Junos Space nodes in the fabric and the VIP address of the fabric may or may not be on the same subnet. The eth1 interface provides SSH access to the Junos Space nodes.

The VIP address and the devices being managed by Junos Space are on the same subnet.

- Configure the eth0, eth1, and eth3 interfaces.

When Ethernet interfaces eth0, eth1, and eth3 are used, the Junos Space nodes in the fabric and the VIP address of the fabric may or may not be on the same subnet. The Junos Space nodes are reachable (SSH access) only through the eth1 interface.

The managed devices can be reached through the eth0 interface if they are configured on the same subnet as the VIP address; on any other subnet, the managed devices can be reached through the eth3 interface.

NOTE: If the managed devices are not reachable through the default gateway configured for the eth3 interface, you must configure static routes for the eth3 interface. The eth3 interface refers to the devint routing table.

Any static route configured manually is populated in the main routing table, which is used to route traffic through the eth0 interface.

- When you configure an appliance as a specialized node used for fault monitoring and performance monitoring (FMPM), you can use only the Ethernet interfaces eth0 and eth1.

Ethernet interface eth1 provides SSH access to FMPM nodes.

NOTE: For more information about the Junos Space fabric, refer to the *Managing Nodes in the Junos Space Fabric* chapter in the *Junos Space Network Management Platform Workspaces Feature Guide* (available at https://www.juniper.net/documentation/en_US/junos-space18.1/index.html).

Table 4 on page 16 summarizes the functions of Ethernet interfaces on the Junos Space Virtual Appliance.

Table 4: Junos Space Virtual Appliance Ethernet Interfaces

Interface	Function
eth0	SSH and device management, if only the Ethernet interface ETH0 or Ethernet interface 0 is used
eth0:0	GUI interface
eth1	SSH access to the Junos Space nodes NOTE: SSH is disabled on the eth0 and eth3 interfaces when eth1 is configured.
eth2	Reserved for future use
eth3	Device management when managed devices are on an out-of-band management subnet and not reachable by the Ethernet interface eth0

RELATED DOCUMENTATION

Configuring a Junos Space Virtual Appliance as a Standalone or Primary FMPPM Node | 70

Changing the Network and System Settings of a Junos Space Virtual Appliance | 89

2

CHAPTER

Deploying the Junos Space Virtual Appliance

Junos Space Virtual Appliance Deployment Overview | 19

Deploying a Junos Space Virtual Appliance on a VMware ESXi Server | 23

Deploying a Junos Space Virtual Appliance on a KVM Server | 28

Adding Disk Resources for a Junos Space Virtual Appliance | 33

Starting Open VM Tools in Junos Space Platform | 37

Installing VI Toolkit for Perl on Junos Space Virtual Appliance | 39

Junos Space Virtual Appliance Deployment Overview

The Junos Space Virtual Appliance is distributed in the Open Virtualization Appliance (OVA) and qcow2 formats.

You can deploy the Junos Space Virtual Appliance *.ova file on a VMware ESXi server version 5.5, 6.0, or 6.5 and the *.qcow2 on a Kernel-based Virtual Machine (KVM) server. The Junos Space Virtual Appliance Release 16.1R1 and later can be deployed on qemu-kvm (KVM) Release 1.5.3-105.el7 or later which runs on CentOS Release 7.2. From Junos Space Network Management Platform Release 18.2 onward, Junos Space Virtual Appliance will be installed with VM Hardware version 8.

NOTE: Though a KVM server on other Linux distributions is supported, we recommend that you use KVM on CentOS.

After the Junos Space Virtual Appliance is deployed, you can use the VMware vSphere client or Virtual Machine Manager (VMM) to connect to the VMware ESX (or VMware ESXi) server or KVM server respectively and configure the Junos Space Virtual Appliance.

The minimum hardware requirements for deploying a Junos Space Virtual Appliance are as follows:

- 64-bit quad processor with a clock speed of at least 2.66 GHz
- Four virtual CPUs
- 1-Gbps network
- 32-GB RAM to configure the virtual appliance as a Junos Space node or fault monitoring and performance monitoring (FMPM) node

NOTE: 64-GB RAM is required if the number of rules per firewall (SRX) cluster is more than 6000 and if firewall policies of similar sizes are being concurrently published.

- 500-GB hard disk

Ensure that 100-GB free disk space is available if the Junos Space Virtual Appliance is to be configured as a FMPM node. For information about adding disk resources, refer to [“Adding Disk Resources for a Junos Space Virtual Appliance” on page 33](#).

- 1-TB hard disk if you are configuring Database nodes
- Configure Open VM tools (see [“Starting Open VM Tools in Junos Space Platform” on page 37](#) for details.)

NOTE:

- We recommend that you use disks with I/O speed of 200 MBps or above. For information about determining I/O speed of a disk used in the node of a Junos Space cluster, see *How do I Determine the Disk I/O Speed of a Node in the Junos Space Fabric?* in the [Junos Space Hardware and Virtual Appliances FAQ](#).
- We recommend against cloning a deployed Junos Space Image and using it as another instance of a Junos Space Virtual Appliance.

Table 5 on page 20 shows the ports that are open on Junos Space Virtual Appliance and the corresponding utilization of these open ports.

Table 5: Open Ports Utilization Matrix

Port Number	Protocol	Process	Description
2050	UDP	Python AV-EMB-CONFIG	View application tokens that allow Security Director or OpenAPI users to securely access Juniper SkyATP APIs over HTTPS. <ul style="list-style-type: none"> • Port 2050 (UDP)—Used to receive attack packets sent by SRX Series devices. • Port 2051 (TCP)—Used by Security Director to fetch the attack packets stored in Junos Space Network Management Platform database.
3000	TCP	node slipstream-hbci	Security Director application uses Juniper Networks's in-house user interface (UI) framework called Slipstream. The Slipstream framework runs on a light weight web server called Node.js listening on the port 3000. All the UI requests from Security Director goes to Node.js server and it is redirected to internal JBoss-EJB layer for business logic.
3151	TCP	Python - NetMike Assessor	Security Director runs a Python-based web server listening on the 3151 port for VPN monitoring.

Table 5: Open Ports Utilization Matrix (continued)

Port Number	Protocol	Process	Description
6234	TCP	JUNIPER-SKYATP-CRONJOBS	<p>Policy Enforcer, a component of the Junos Space Security Director user interface, integrates with Juniper Sky ATP to provide centralized threat management and monitoring to your software-defined secure network, giving you the ability to combine threat intelligence from different solutions and act on that intelligence from one management point. For example, if a user downloads a file from the Internet and that file passes through an SRX Series firewall, the file can be sent to the Juniper Sky ATP cloud for malware inspection.</p> <p>The 6234 port is used for Sky ATP proxy.</p>
45688	UDP	JGROUPS for Multicast	<p>Junos Space uses JBoss application server as a underlying server. JGroups is a library for reliable one-to-one or one-to-many communication, which is used by JBoss application server to form the Junos Space clustering and interchange the message or data between the cluster nodes and failure detections. JBoss uses internal data cache to store the common data across the cluster node, and the data is replicated across cluster node through this multicast port.</p>
54200-54249	TCP	JBOSS-JGROUPS-FailureDetection	<p>Junos Space uses JBoss application server as a underlying server. JGroups is a library for reliable one-to-one or one-to-many communication, which is used by JBoss application server to form the Junos Space clustering and interchange the message or data between the cluster nodes and failure detections. TCP stack is used for the unicast communication that is, a direct communication between the Junos Space cluster nodes.</p>
55200	UDP	JGROUPS UDP stack	Security Director uses the 55200 port.

Table 5: Open Ports Utilization Matrix (continued)

Port Number	Protocol	Process	Description
55200-55249	UDP	JBOSS-JGROUPS	Junos Space uses JBoss application server as a underlying server. JGroups is a library for reliable one-to-one or one-to-many communication, which is used by JBoss application server to form the Junos Space clustering and interchange the message or data between cluster nodes. UDP stack is used for multicast communication.
54200-54211	TCP	JGROUPS for Failure Detection (FD)	
57225	UDP	JBOSS-AS	
10164	UDP	JBOSS-AS	Security Director uses the 10164 port to receive the SNMP Trap alerts from the SRX Series devices. It is primarily for Security Director Fault management capability.
694	UDP	Linux-HA high-availability heartbeat	Security Director uses the 694 port to receive high-availability heartbeat.
3306	TCP	MySQL database system	Security Director uses the 3306 port.
4447	TCP	N1-RMGMT	Security Director uses the 4447 port.
5432	TCP	Postgre SQL database system	Security Director uses the 5432 port.
5445	TCP	Server Message Block over Remote Direct Memory Access	Security Director uses the 5445 port.
7804	TCP	Inbound to the Junos Space server nodes IP	Security Director uses the 7804 port.
8009	TCP	Apache JServ Protocol (ajp13)	Security Director uses the 8009 port.
8080	TCP	Apache Tomcat	Security Director uses the 8080 port.
8101	TCP	Logical Domains Migration	Used by OpenNMS and Security Director.
8888	TCP	Default for IPython , HyperVM over HTTPS	Security Director uses the 8888 port.

Table 5: Open Ports Utilization Matrix (*continued*)

Port Number	Protocol	Process	Description
9200	TCP	Elastic search	This is the default elastic search port used by Security Director.
9300	TCP	Virtual Racing Service - Elastic Search	Security Director uses the 9300 port.
9876	TCP	Session Director - Multicast	Security Director uses the 9876 port.
9999	TCP	JBoss Management (Administration)	Security Director uses the 9876 port.
11099	TCP	Used by OpenNMS	Security Director uses the 11099 port.
23364	UDP	MODCLUSTER - multicasting - HTTPD Service	Security Director uses the 23364 port.

RELATED DOCUMENTATION

[Deploying a Junos Space Virtual Appliance on a VMware ESXi Server | 23](#)
[Deploying a Junos Space Virtual Appliance on a KVM Server | 28](#)
[Adding Disk Resources for a Junos Space Virtual Appliance | 33](#)

Deploying a Junos Space Virtual Appliance on a VMware ESXi Server

The Junos Space Virtual Appliance requires a VMware ESXi server 5.5, 6.0, or 6.5 that can support a virtual machine with the following configuration:

NOTE:

- The ESXi host server must include a Standard or Enterprise edition license, which may not be installed on the host server by default.
- VMware VMotion is supported for moving Junos Space Virtual Appliances from one VMware ESXi server to another VMware ESXi server.

For information about the minimum hardware requirements for deploying a Junos Space Virtual Appliance, see “[Junos Space Virtual Appliance Deployment Overview](#)” on page 19.

BEST PRACTICE: We recommend the following best practices after you deploy the Junos Space Virtual Appliance on a VMWare ESXi server:

- VMWare ESXi server snapshots should be taken after shutting down Junos Space servers. Ensure snapshots are taken simultaneously across all the nodes in the fabric.
- To ensure optimal performance of Junos Space, configure purging policies for the VMWare host one month after the Junos Space fabric is functional.

The deployment of a Junos Space Virtual Appliance on a VMware ESXi server includes the following tasks:

1. [Installing the VMware ESXi Server | 24](#)
2. [Installing a Junos Space Virtual Appliance on a VMware ESXi Server | 25](#)
3. [Modifying RAM Settings for a Junos Space Virtual Appliance | 27](#)
4. [Adding Disk Resources for a Junos Space Virtual Appliance | 28](#)

Installing the VMware ESXi Server

To install the VMware ESXi server:

1. Download the VMware ESXi server installation package from <https://www.vmware.com/download/vi/>.
2. Install the VMware ESXi server.

For instructions to install the VMware ESXi server, go to https://www.vmware.com/support/pubs/vi_pubs.html.

NOTE: You can install the VMware vSphere Client when you install the VMware ESXi server 5.5, 6.0, or 6.5. Contact VMware for support with installing ESXi server.

NOTE: Junos Space Network Management Platform is not certified to be used with VMware tools.

Installing a Junos Space Virtual Appliance on a VMware ESXi Server

IN THIS SECTION

- Installing a Junos Space Virtual Appliance by Using vSphere Client | 25
- Installing a Junos Space Virtual Appliance by Using the OVF Tool | 26

You can use vSphere Client 4.0 or later or OVF Tool 2.01 or later to deploy the Junos Space Virtual Appliance image on a VMWare ESXi server.

Installing a Junos Space Virtual Appliance by Using vSphere Client

To create a Junos Space Virtual Appliance by using vSphere Client 4.0:

1. Download the Junos Space Virtual Appliance image from <https://www.juniper.net/support/downloads/?p=space#sw> to your local system.

NOTE: Do not change the name of the Junos Space Virtual Appliance image file that you download from the Juniper Networks support site. If you change the name of the image file, the creation of the Junos Space Virtual Appliance can fail.

2. Launch the vSphere Client that is connected to the ESXi server where the Junos Space Virtual Appliance is to be deployed.
3. Select **File > Deploy OVF Template** from the menu bar.
The Deploy OVF Template page appears.
4. Click the **Deploy from file** option and click **Browse**, and then upload the OVA file from your storage location.

NOTE: You can use the same image to deploy both Junos Space and fault monitoring and performance monitoring (FMPM) nodes.

5. Click **Next**.

6. Verify the OVF Template details and then click **Next**.

7. Specify a name and location for the deployed template and then click **Next**.

A template name can contain a maximum of 80 characters. Template names are not case-sensitive.

8. Verify your settings and then click **Finish** to create the Junos Space Virtual Appliance.

Installing a Junos Space Virtual Appliance by Using the OVF Tool

Before you use the OVF Tool to create a Junos Space Virtual Appliance, ensure that the OVF Tool is installed on the system where you save the Junos Space Virtual Appliance image file (*.ova).

To create a Junos Space Virtual Appliance by using the OVF Tool:

1. Download the Junos Space Virtual Appliance image from <https://www.juniper.net/support/downloads/?p=space#sw> to your local system.

NOTE: Do not change the name of the Junos Space Virtual Appliance image file that you download from the Juniper Networks support site. If you change the name of the image file, the creation of the Junos Space Virtual Appliance can fail.

2. Log in to the local system and navigate to the location where the Junos Space Virtual Appliance image file is saved.

3. Run the following command:

```
/usr/bin/ovftool/ovftool --name=virtual-appliance image-file
vi://username:password@host-id
```

where:

- *virtual-appliance* is the name you assign to the Junos Space Virtual Appliance.
- *image-file* is the name of the Junos Space Virtual Appliance image file.
- *username* is the username of the host machine where you deploy the Junos Space Virtual Appliance.
- *password* is the password of the host machine where you deploy the Junos Space Virtual Appliance.
- *host-id* is the IP address of the host machine where you deploy the Junos Space Virtual Appliance.

Example:

```
/usr/bin/ovftool/ovftool -name=space1vm space-19.3R1.0.ova
vi://username:password@10.157.10.1
```

The Junos Space Virtual Appliance is deployed on the host machine.

4. Log in to the host machine and edit the settings (number of processors, memory) of the Junos Space Virtual Appliance. For information about editing the settings of a Junos Space Virtual Appliance by using the OVF Tool, see the OVF Tool documentation at <https://www.vmware.com/support/developer/ovf/>.

Modifying RAM Settings for a Junos Space Virtual Appliance

To add RAM for a Junos Space Virtual Appliance:

1. Launch the VMware vSphere Client and log in to the ESXi server where the Junos Space Virtual Appliance is deployed.
2. Select the Junos Space Virtual Appliance from the inventory view.
3. If the Junos Space Virtual Appliance is powered on, you must power off the appliance to configure RAM.

To power off the Junos Space Virtual Appliance, right-click the Junos Space Virtual Appliance icon and select **Power > Power Off**.

4. Select the **Summary** tab to view the Junos Space virtual machine settings.
5. Select **Edit Settings** to view and edit the virtual memory settings.
6. Select **Memory**.
7. Update the RAM to 32 GB to operate the Junos Space Virtual Appliance as a Junos Space node or as an FMPM node.
8. Click **OK**.

RAM is added to the Junos Space Virtual Appliance.

Adding Disk Resources for a Junos Space Virtual Appliance

For information about adding disk resources for Junos Space Virtual Appliance, see [“Adding Disk Resources for a Junos Space Virtual Appliance” on page 33](#).

RELATED DOCUMENTATION

[Configuring a Junos Space Virtual Appliance as a Junos Space Node | 43](#)

[Configuring a Junos Space Virtual Appliance as a Standalone or Primary FMPM Node | 70](#)

[Configuring a Junos Space Virtual Appliance as a Backup or Secondary FMPM Node for High Availability | 81](#)

[Adding a Node to an Existing Junos Space Fabric | 141](#)

[Viewing Nodes in the Fabric | 150](#)

Deploying a Junos Space Virtual Appliance on a KVM Server

The Junos Space Virtual Appliance Release 16.1R1 and later can be deployed on qemu-kvm (KVM) Release 1.5.3 or later.

NOTE: Juniper Networks does not provide any support for installing and configuring the KVM server. You must install the virtual appliance image and configure it as per the recommended specifications for the virtual appliance. Juniper Networks will provide support only after the Junos Space Virtual Appliance has booted successfully.

The prerequisites to deploy a Junos Space Virtual Appliance on a KVM server are as follows:

- Knowledge about configuring and installing a KVM server.
- KVM server and supported packages must be installed on your Linux-based system. Contact your Linux vendor or documentation for information about installing KVM.
- An application or method to view the remote system virtual monitor, such as Virtual Machine Manager (VMM), Virtual Network Computing (VNC) Viewer, or any other application.
- Bridge Interface configured according to your environment and at least two free static IP addresses.

For information about the minimum hardware requirements for deploying a Junos Space Virtual Appliance, see “[Junos Space Virtual Appliance Deployment Overview](#)” on page 19.

The deployment of a Junos Space Virtual Appliance on a KVM server by using VMM includes the following tasks:

NOTE: Though deploying the Junos Space Virtual Appliance on the KVM server by using virtual machine clients other than VMM is possible, Juniper Networks does not provide support for installing the Junos Space Virtual Appliance using clients other than VMM.

1. [Installing a Junos Space Virtual Appliance on the KVM Server by Using VMM](#) | 29
2. [Modifying the Type of Virtual Disk Interface](#) | 31
3. [Modifying RAM for a Junos Space Virtual Appliance](#) | 32
4. [Adding Disk Resources for a Junos Space Virtual Appliance](#) | 32
5. [Enabling Multicast on Bridged Interfaces of a KVM-Host Machine](#) | 32

Installing a Junos Space Virtual Appliance on the KVM Server by Using VMM

Use the VMM virtual machine client to install the Junos Space Virtual Appliance on a KVM server.

To install the Junos Space Virtual Appliance on a KVM server by using VMM:

1. Download the Junos Space Virtual Appliance image from <https://www.juniper.net/support/downloads/?p=space#sw> to your local system.

NOTE: Do not change the name of the Junos Space Virtual Appliance image file that you download from the Juniper Networks support site. If you change the name of the image file, the creation of the Junos Space Virtual Appliance can fail.

2. Launch the VMM client.
3. Select **File > New Virtual Machine** on the menu bar of VMM to install a new virtual machine on a KVM server.

The New VM dialog box appears and displays Step 1 of 4 of the New VM installation.

4. Under Choose how you would like to install the operating system, click **Import existing disk image**.

5. Click **Forward** to go to the next step.

Step 2 of 4 is displayed.

6. Under Provide the existing storage path, click **Browse**.

7. Under Choose storage volume , click **Browse Local** at the bottom of the dialog box to locate and select the Junos Space Virtual Appliance image file (**.qcow2**) saved on your system.

8. Under Choose an operating system type and version, select Linux for **OS type** and Red Hat Enterprise Linux *version number* for **Version**.

NOTE: We recommend to use the same Linux version as Junos Space Platform is using.

9. Click **Forward** to go to the next step.

Step 3 of 4 is displayed.

10. Under Choose Memory and CPU settings, ensure that 4 is set for **CPUs** and select or enter the following value for **Memory (RAM)**:

- 32768 MB–For the Junos Space Virtual Appliance to be deployed as a Junos Space node or as an FMPM node

11. Click **Forward** to go to the next step.

Step 4 of 4 is displayed.

12. Under Ready to begin the installation, in the Name field, enter a name for the Junos Space Virtual Appliance.

13. Under Network selection, select the options based on how you want to configure network communication on the Junos Space Platform setup.

14. Click **Finish**.

The New VM dialog box closes. The Junos Space Virtual Appliance is started and the console is displayed.

The Junos Space Virtual Appliance is created and listed with the name that you entered in the VMM.

Modifying the Type of Virtual Disk Interface

After the Junos Space Virtual Appliance is created, you must change the hard disk interface type to Integrated Drive Electronics (IDE) to avoid any issues with the booting up of the Junos Space Virtual Appliance due to kernel panic.

NOTE: If you are using CLI of VMM to set up KVM, you set the type of virtual disk interface to IDE at the start of the set up. You do not have to reset the type of interface again.

To change the hard disk interface type to IDE:

1. Select the Junos Space Virtual Appliance just created and select **Edit > Virtual Machine Details** on the menu bar of VMM to edit the hardware settings.
2. Click the **Show virtual hardware details** icon in the Virtual Machine Details dialog box.
3. Click **VirtIO Disk1 (Virtual Disk)** on the left of the dialog box to change the type of the disk interface to IDE.

The details of the Virtual disk is displayed on the right of the dialog box.

4. Under Advanced Options, select IDE for **Disk Bus** and qcow2 for **Storage format**.
5. Click **Apply**.
6. (Optional) To apply the changes immediately, shut down and restart the virtual appliance if the Junos Space Virtual Appliance is already powered on.

To restart the Junos Space Virtual Appliance:

- a. Right-click the Junos Space Virtual Appliance icon and select **Shutdown > Power Off**, to shut down the Junos Space Virtual Appliance.
- b. Select the Junos Space Virtual Appliance icon and click the **Power on the virtual machine** icon to start the Junos Space Virtual Appliance. Alternatively, you can right-click the Junos Space Virtual Appliance icon and select **Run**.

Modifying RAM for a Junos Space Virtual Appliance

The Junos Space Virtual Appliance file is distributed with 8 GB of RAM and four virtual CPUs. You need 32-GB RAM to configure the Junos Space Virtual Appliance as a Junos Space node or as an FMPM node.

To modify RAM for the Junos Space Virtual Appliance:

1. Launch VMM and select the Junos Space Virtual Appliance for which you want to modify RAM.
2. (Optional) If the Junos Space Virtual Appliance is running, you must shut down the appliance to modify RAM.

To shut down the Junos Space Virtual Appliance, right-click the Junos Space Virtual Appliance icon and select **Shutdown > Power Off**.

3. To view and change RAM allocated to the Junos Space Virtual Appliance, select **Edit > Virtual Machine Details** on the menu bar of VMM to edit the hardware settings.
4. Click the **Show virtual hardware details** icon in the Virtual Machine Details dialog box.
5. Click **Memory** on the left side of the dialog box.

The RAM details of the virtual machine is displayed on the right of the dialog box.

6. Enter the required memory in the **Current allocation** and **Maximum allocation** fields.
7. Click **Apply** to modify the RAM allocation.

Adding Disk Resources for a Junos Space Virtual Appliance

For information about adding disk resources for Junos Space Virtual Appliance, see [“Adding Disk Resources for a Junos Space Virtual Appliance” on page 33](#).

Enabling Multicast on Bridged Interfaces of a KVM-Host Machine

For creating Junos Space clusters, multicast must be enabled on the bridged interface of a KVM-host machine on which Junos Space node is deployed to allow multicast traffic to flow between the nodes of the cluster.. If Junos Space nodes in a cluster are deployed on different host machines, multicast must be enabled on the bridged interface of each host machine.

To configure multicast on a bridged interface of a KVM-host machine, log in to the KVM-host machine after the UI of the Junos Space node is up and execute the **ifconfig *InterfaceName* allmulti** command, where *InterfaceName* is the name of the interface.

Example:

```
-bash-4.1$ ifconfig macvtap0 allmulti
```

NOTE: Configure multicast on all the KVM-host machines before adding a Junos Space node to a cluster.

RELATED DOCUMENTATION

[Configuring a Junos Space Virtual Appliance as a Junos Space Node | 43](#)

[Configuring a Junos Space Virtual Appliance as a Standalone or Primary FMPM Node | 70](#)

[Configuring a Junos Space Virtual Appliance as a Backup or Secondary FMPM Node for High Availability | 81](#)

[Adding a Node to an Existing Junos Space Fabric | 141](#)

[Viewing Nodes in the Fabric | 150](#)

Adding Disk Resources for a Junos Space Virtual Appliance

IN THIS SECTION

- [Adding Disk Resources for a Junos Space Virtual Appliance Deployed on a VMware ESX or VMware ESXi Server | 35](#)
- [Adding Disk Resources for a Junos Space Virtual Appliance Deployed on a KVM Server | 36](#)

The Junos Space Virtual Appliance files are distributed with 250-GB of disk space.

NOTE:

- The free space available in all the partitions should be monitored periodically and the available free disk space increased if required. The **/var** and **/var/log** partitions should be monitored more frequently as most of the data are stored in these partitions and space utilization is high.

For information about disk space needed for installing a Junos Space application, refer to the respective application documentation available at *Junos Space Software, Release 18.3*.

- If you are expanding the disk space of nodes in a Junos Space fabric (cluster) comprising virtual appliances, you must first expand the disk space of the virtual IP (VIP) node and ensure that the VIP node has come up, that is, JBoss and MySQL services are up before expanding the disk space of other nodes in the fabric; otherwise, the fabric may become unstable and the Junos Space GUI inaccessible.
- While configuring a Junos Space Virtual Appliance as a Junos Space node or an FMPM node, it is recommended that you allocate disk space partitions as per the disk space allocations for a JA2500 Junos Space Appliance. However, you can allocate less or more space to disk partitions as per your requirement. For more information about disk space allocation in JA2500 Junos Space Appliance, see [Configuring a Junos Space Appliance as a Junos Space Node](#).

To allocate additional disk space for partitions, add a disk resource and expand a partition one at a time. The free space available on the disk resource can be shared among the different partitions. For example, to expand the **/var** and **/var/log** partitions by 20 GB each, add a disk resource of minimum 40 GB. Expand the drive size of the **/var** partition by 20 GB and then expand the **/var/log** partition by 20 GB.

[Table 6 on page 34](#) specifies the data stored in the partitions of a Junos Space Node and an FMPM node.

Table 6: Data Stored in the Partitions of a Junos Space Node and an FMPM Node

Partition	Junos Space Node	FMPM Node
/var	MySQL database, PostgreSQL database, database backup file, and disaster recovery data files	FMPM data, MySQL database, PostgreSQL database
/var/log	All system log files	All system log files
/tmp	Temporary files	Temporary files
/	Worldwide adapters, JBoss configuration files	OpenNMS installation

The following tasks that must be performed for adding disk resources are explained in this topic:

Adding Disk Resources for a Junos Space Virtual Appliance Deployed on a VMware ESX or VMware ESXi Server

The Junos Space Virtual Appliance file is distributed with 250 GB of disk space. You can increase the hard disk size based on the requirement for the specific Junos Space deployment. The following procedure describes how you can add disk resources for a Junos Space Virtual Appliance deployed on a VMware ESX or VMware ESXi Server.

To add disk resources for the Junos Space Virtual Appliance:

1. In the VMware vSphere Client, right-click the Junos Space Virtual Appliance icon and select **Power > Power On**. The Junos Space Virtual Appliance must be powered on to add disk resources.

2. Right-click the Junos Space Virtual Appliance icon and select **Edit Settings**.

The Virtual Machine Properties page is displayed.

3. Select the Hardware tab and click **Add**.

The Device Type page is displayed.

4. Under Choose the type of disk you wish to add, select **Hard Disk**.

5. Click **Next**.

The Select a Disk page appears.

6. Under Disk, select **Create a new Virtual disk**.

7. Click **Next**.

The Create a Disk page appears.

8. Under Capacity, set the Disk Size field to the recommended size for the partition that you want to expand.

Under Location, retain the default setting—that is, leave the **Store with the virtual machine** selected.

9. Click **Next**.

The Advanced Options page is displayed.

10. Leave the default settings unchanged and click **Next**.

The Ready to Complete page is displayed.

11. Review your selected options and click **Finish**.

The Virtual Machine Properties page displays the new virtual disk on the Hardware list.

12. Click **OK** to create the new virtual disk.

A status bar shows the progress at the bottom of the page.

The next step is to configure the basic settings for your deployed Junos Space Virtual Appliance. To configure basic settings for the appliance, access the console in the VMware vSphere Client.

NOTE: After the new virtual disk is created, the Junos Space Virtual Appliance must be scanned to detect the additional disk space that you added. To start the scan for additional disk space, select the **Expand VM Drive Size** option from the Junos Space Settings Menu immediately after you configure the basic settings for your Junos Space Virtual Appliance.

For information about expanding the drive size, refer to [“Configuring a Junos Space Virtual Appliance as a Junos Space Node” on page 43](#).

Adding Disk Resources for a Junos Space Virtual Appliance Deployed on a KVM Server

The Junos Space Virtual Appliance file is distributed with 250 GB of disk space. You can increase the size of the hard disk based on the requirement for the specific Junos Space deployment. The following procedure describes how you can add disk resources for a Junos Space Virtual Appliance deployed on a KVM Server.

To add disk resources for the Junos Space Virtual Appliance:

1. Launch VMM and select the Junos Space Virtual Appliance for which you want to modify the disk space.
2. Select **Edit > Virtual Machine Details** on the menu bar of VMM to edit the hardware settings.
3. Click the **Show virtual hardware details** icon in the Virtual Machine Details dialog box.
4. Click **Add Hardware** at the bottom left of the dialog box.

The Add New Virtual Hardware dialog box is displayed.

5. Click **Storage**, select **Create a disk image for the virtual machine**, and enter the required disk space in the box.
6. Select IDE for **Bus Type**.
7. Click **Finish**.

You can see the newly-added disk listed in the left pane.

8. (Optional) If the Junos Space Virtual Appliance is already powered on, shut down and restart the Virtual appliance.

To restart the Junos Space Virtual Appliance:

- a. Right-click the Junos Space Virtual Appliance icon and select **Shutdown > Power Off**, to shut down the Junos Space Virtual Appliance.
- b. Select the Junos Space Virtual Appliance icon and click the **Power on the virtual machine** icon to start the Junos Space Virtual Appliance. Alternatively, you can right-click the Junos Space Virtual Appliance icon and select **Run**.

RELATED DOCUMENTATION

[Changing the Network and System Settings of a Junos Space Virtual Appliance | 89](#)

[Configuring a Junos Space Virtual Appliance as a Junos Space Node | 43](#)

[Configuring a Junos Space Virtual Appliance as a Standalone or Primary FMPM Node | 70](#)

[Configuring a Junos Space Virtual Appliance as a Backup or Secondary FMPM Node for High Availability | 81](#)

Starting Open VM Tools in Junos Space Platform

Junos Space Network Management Platform Release 16.1R1 supports the use of Open VM Tools to facilitate better management and the seamless interaction of the VMware ESXi 6.0 server with the Junos Space Virtual Appliance.

NOTE: Before you start Open VM Tools in Junos Space Platform, ensure that you have installed Open VM Tools 10.1.5 on the Junos Space Virtual Appliance.

You need the following utilities and drivers to build the Open VM Tools—xmlsec1, xmlsec1-openssl, libmspack, libdnet, libicu, fuse-libs, and fuse. Download these utilities and drivers from <https://fedoraproject.org/wiki/EPEL> or https://dl.fedoraproject.org/pub/epel/6/x86_64/Packages/o/open-vm-tools-10.1.5-6.el6.x86_64.rpm.

To start Open VM Tools in Junos Space Platform:

1. Log in to the Junos Space Virtual Appliance as the admin user.

The Junos Space Settings menu is displayed.

2. Type **7** to access the shell.

You are prompted to enter the administrator password.

3. Type the administrator password and press Enter.

The shell prompt appears, as shown in the following example:

```
[user@host ~]#
```

4. Type the **/usr/bin/vmtoolsd &** command at the shell prompt and press Enter:

```
[user@host ~]# /usr/bin/vmtoolsd &
```

The Open VM Tools service is started on the node.

NOTE: To start Open VM Tools each time the Junos Space node is rebooted, add the **/usr/bin/vmtoolsd &** command to the **/etc/rc.local** file.

Release History Table

Release	Description
16.1R1	Junos Space Network Management Platform Release 16.1R1 supports the use of Open VM Tools to facilitate better management and the seamless interaction of the VMware ESXi 6.0 server with the Junos Space Virtual Appliance

RELATED DOCUMENTATION

[Junos Space Virtual Appliance Deployment Overview](#) | 19

Installing VI Toolkit for Perl on Junos Space Virtual Appliance

You can install VMware Infrastructure Toolkit (VI Toolkit) on a Junos Space virtual appliance deployed on a VMware Elastic Sky X (ESX) server or an ESXi server to enable the System Snapshot feature in Junos Space Network Management Platform.

The System Snapshot feature enables you to create a snapshot of the system state and roll back the system to a predefined state.

NOTE: If you have a fabric consisting of only virtual appliances, then VI Toolkit for Perl must be installed on all nodes of the fabric for the System Snapshot functionality to be enabled on Junos Space Platform.

To install VI Toolkit for Perl on a Junos Space virtual appliance deployed on an ESX or an ESXi server:

1. Open <https://www.vmware.com/support/developer/viperltoolkit/> in a web browser.

The VMware vSphere SDK for Perl Documentation page is displayed.

2. Select the release **VI Perl Toolkit 1.6** from the drop-down list.

3. Click the **Download** link.

You are redirected to the VMware login page.

4. If you are not a registered user, click **Register**.

You are redirected to the registration page. Follow the prompts on the registration page and activate your account.

5. Log in using your VMware credentials.

The VMware Infrastructure Perl Toolkit page opens, displaying a list of different packages of VI Perl Toolkit 1.6.

6. From the list, click the **Download Now** button for the **VMware-VIPerl-1.6.0-104313.x86_64.tar.gz** (VI Perl Toolkit - Linux Installer for 64-bit) package.

The End User License Agreement dialog box is displayed.

7. Follow the prompts displayed on the page to download the file.

The **VMware-VIPerl-1.6.0-104313.x86_64.tar.gz** file is downloaded to your local computer.

8. Connect to the Junos Space node (by using SSH) and log in (as the **admin** user) to access the Junos Space CLI.

9. Open a debug (command) prompt by using the Junos Space Settings menu.

10. Create a new directory named **jmp-vm** by executing the following command:

```
mkdir /usr/local/jmp-vm
```

11. Copy the **VMware-VIPerl-1.6.0-104313.x86_64.tar.gz** file you downloaded to the directory **/usr/local/jmp-vm**.

12. Change the current directory to **/usr/local/jmp-vm** by executing the following command:

```
cd /usr/local/jmp-vm
```

13. Extract the compressed TAR files by executing the following command:

```
tar -zxvf *.gz
```

14. Create a new directory named **etc** within the folder **vmware-viperl-distrib** by executing the following command:

```
mkdir /usr/local/jmp-vm/vmware-viperl-distrib/etc
```

15. Copy the file **vmware-uninstall-viperl.pl** from the directory **/var/www/cgi-bin** to the directory named **/usr/local/jmp-vm/vmware-viperl-distrib/bin** on the local machine by using the following command:


```
cp /var/www/cgi-bin/vmware-uninstall-viperl.pl
/usr/local/jmp-vm/vmware-viperl-distrib/bin/vmware-uninstall-viperl.pl
```

The following message is displayed:

```
cp: overwrite /usr/local/jmp-vm/vmware-viperl-distrib/bin/vmware-uninstall-viperl.pl?
```

16. Type **yes** to replace the existing **vmware-uninstall-viperl.pl** file and press Enter.

17. Change the permissions of the files in the **/usr/local/jmp-vm** folder to allow read and execute permissions to everyone and, additionally, write permission to the file owner by executing the following command:

```
chmod -R 755 /usr/local/jmp-vm
```

18. Run the file **vmware-install.pl** by executing the following command:

```
perl vmware-viperl-distrib/vmware-install.pl --prefix=1
```

On successful installation, the following message is displayed:

The installation of VMware VIPerl Toolkit 1.6.0 build-104313 for Linux completed successfully. You can decide to remove this software from your system at any time by invoking the following command: "1/bin/vmware-uninstall-viperl.pl"

19. Log out of the Junos Space VIP node.

You can now create a System Snapshot by going to the Fabric page (**Administration > Fabric**). For more information, see *Creating a System Snapshot*.

RELATED DOCUMENTATION

Creating a System Snapshot

[Junos Space Virtual Appliance Deployment Overview | 19](#)

[Configuring a Junos Space Virtual Appliance as a Junos Space Node | 43](#)

3

CHAPTER

Configuring the Junos Space Virtual Appliance

Configuring a Junos Space Virtual Appliance as a Junos Space Node | **43**

Configuring a Junos Space Virtual Appliance as a Standalone or Primary FMPM Node | **70**

Configuring a Junos Space Virtual Appliance as a Backup or Secondary FMPM Node for High Availability | **81**

Changing the Network and System Settings of a Junos Space Virtual Appliance | **89**

Configuring a Junos Space Virtual Appliance as a Junos Space Node

After you deploy a Junos Space Virtual Appliance on a VMware ESX, VMware ESXi, or Kernel-based Virtual Machine (KVM) server, you must enter basic network and machine information to make your Junos Space Virtual Appliance accessible on the network. You must also add disk space to the partitions of the Junos Space Virtual Appliance.

NOTE:

- From Junos Space Network Management Platform Release 14.1R2 onward, you can configure Junos Space Ethernet interfaces with only IPv4 addresses, or both IPv4 and IPv6 addresses.
- From Junos Space Network Management Platform Release 16.1R1 onward, you can configure access to Junos Space through a Network Address Translation (NAT) gateway.

Before you begin, ensure that you have the following information available:

- IPv4 address and subnet mask for the node management (eth0) Ethernet interface
- (Optional) IPv6 address and prefix for the eth0 Ethernet interface
- IPv4 address of the default gateway for the eth0 Ethernet interface
- (Optional) IPv6 address of the default gateway for the eth0 Ethernet interface
- IPv4 address of the name server
- (Optional) IPv6 address of the name server
- (Optional) IPv4 address and subnet mask for the Ethernet interface eth3, if you are configuring a device management interface.

NOTE: When you configure the eth3 interface as the device management interface, the IP addresses of the eth0 and eth3 Ethernet interfaces must be in different subnets.

- (Optional) IPv4 address of the default gateway for the eth3 Ethernet interface

NOTE: If you configure the IPv4 address for the eth3 Ethernet interface, you must configure the IPv4 address of the default gateway.

- (Optional) IPv6 address and prefix for the eth3 Ethernet interface

- (Optional) IPv6 address of the default gateway for the eth3 Ethernet interface

NOTE: If you configure the IPv6 address for the eth3 Ethernet interface, you must configure the IPv6 address of the default gateway for the eth3 interface.

- Virtual IP (VIP) address in IPv4 and IPv6 formats

The IPv4 format of the VIP address is used for accessing the Junos Space Network Management Platform GUI through a Web browser. This IP address must be in the same subnet as the IP address assigned to the eth0 Ethernet interface

The IPv6 format of the VIP address is used for receiving SNMP traps from managed devices.

- IPv4 address or URI of the NTP source to synchronize time

- (Optional) IPv4 address of the eth1 Ethernet interface

If the IP address of the eth1 interface is not in the same subnet as the VIP address, ensure that you have the subnet mask and the default gateway for the eth1 interface.

- (Optional) IPv4 address for the NAT outbound SSH
- (Optional) IPv6 address for the NAT outbound SSH
- (Optional) IPv4 port number for the NAT outbound SSH
- (Optional) IPv6 port number for the NAT outbound SSH
- (Optional) IPv4 address for the NAT trap
- (Optional) IPv6 address for the NAT trap
- (Optional) IPv4 port number for the NAT trap
- (Optional) IPv6 port number for the NAT trap

This topic discusses the following tasks:

- [Configuring a Junos Space Virtual Appliance | 45](#)
- [Configuring Access to Junos Space Through a NAT Gateway | 62](#)
- [Configuring the eth1 Ethernet Interface | 68](#)

Configuring a Junos Space Virtual Appliance

You can configure a Junos Space Virtual Appliance as the first or standalone node in a cluster or add the node to an existing cluster.

To configure a Junos Space Virtual Appliance:

1. Using a virtual machine client (such as VMware vSphere Client or Virtual Machine Manager [VMM]), log in and power on the Junos Space Virtual Appliance.
2. Access the console on the virtual machine client to view the Junos Space login prompt.
3. At the Junos Space login prompt, type **admin** as your default login name and press Enter.

```
space-node login:admin
Password:
```

You are prompted to enter the administrator password.

4. Type **abc123** as the default administrator password and press Enter.

Junos Space prompts you to change your default password.

5. To change the default password, do the following:

- Type the default password and press Enter.
- Type your new password and press Enter.
- Retype your new password and press Enter.

If the password is changed successfully, the following message is displayed.

```
passwd: all authentication tokens updated successfully
```

NOTE: You can choose a password that is at least eight characters long and contains characters from at least three of the following four character classes: uppercase letters, lowercase letters, numbers (0 through 9), and special characters.

However, if a password satisfies the preceding criteria but contains only a single uppercase letter at the beginning or only a single number at the end, then that password is considered invalid. For example, Abcdwip9, Qc9rdiwt, and bRfjvin9 are invalid passwords, but AAbcdwip99, Qc9rdiwtQ, and bRfjvin99 are valid passwords.

Alternatively, instead of using a string of characters, you can choose a passphrase that is between 16 and 40 characters long and contains at least three dictionary words separated by at least one special character. For example, big#three;fork (14 characters long) and circlefaceglass (no special characters) are invalid passphrases, but @big#three;fork& and circle;face;glass are valid passphrases.

Passwords and passphrases are case-sensitive.

6. Enter the new password to log in to Junos Space.
7. Type **S** to install the virtual appliance as a Junos Space node.

This Junos Space node can be installed as one of the following:

(S)pace Platform

Full functionality. Every Junos Space Installation requires at least one Space node.

(F)MPM

Specialized to fault and performance monitoring only. This requires at least one Space node.

Choose the type of node to be installed [S/F] S

8. Configure the IP address for the eth0 interface.

Configuring Eth0:

1> Configure IPv4

2> Configure Both IPv4 and IPv6

```
R> Redraw Menu
```

```
Choice [1-2,R]:
```

- To configure the IPv4 address of the eth0 interface:
 - a. Type **1**.
 - b. Type the IPv4 address for eth0 interface in dotted-decimal notation and press Enter.

```
Please enter new IPv4 address for interface eth0:
192.0.2.50
```

NOTE: All nodes that you configure in a cluster (fabric) must be in the same subnet.

- c. Type the subnet mask for the IPv4 address and press Enter.

```
Please enter new IPv4 subnet mask for interface eth0:
255.255.0.0
```

- d. Type the IPv4 address of the default gateway for the eth0 Ethernet interface in dotted-decimal notation and press Enter.

```
Enter the default IPv4 gateway as a dotted-decimal IP Address:
192.0.2.150
```

- To configure both IPv4 and IPv6 addresses:
 - a. Type **2**.
 - b. Type the IPv4 address for the eth0 interface in dotted-decimal notation and press Enter.

```
Please enter new IPv4 address for interface eth0
192.0.2.50
```

- c. Type a subnet mask for the IPv4 address in dotted-decimal notation and press Enter.

```
Please enter new IPv4 subnet mask for interface eth0:
255.255.0.0
```

- d. Type the IPv4 address of the default gateway for the eth0 interface in dotted-decimal notation and press Enter.

```
Enter the default IPv4 gateway as a dotted decimal IP Address:
192.0.2.150
```

- e. Type the IPv6 address and prefix for the eth0 interface and press Enter.

```
Please enter new IPv6 address with prefix (IPv6 Address/prefix) for interface
eth0:
2001:db8:0:1:192:0:2:50/64
```

NOTE: If you configure an IPv6 address for the eth0 interface, you must also configure an IPv6 address for the name server.

- f. Type the IPv6 address of the default gateway for the eth0 interface and press Enter.

```
Enter the IPv6 gateway:
2001:db8:0:1:192:0:2:150
```

9. Type the IPv4 address of the name server for the eth0 interface and press Enter.

```
Please type the IPv4 nameserver address in dotted decimal notation:
192.0.2.10
```

10. Type the IPv6 address of the name server for the eth0 interface and press Enter.

```
Please type the IPv6 nameserver address:
2001:db8:0:1:192:0:2:10
```

11. Specify whether you want to configure the eth3 Ethernet interface.

Configure a separate interface for device management? [y/n]

NOTE:

- On a Junos Space fabric with two or more Junos Space nodes, if you configure the eth3 interface as the device management interface on one Junos Space node, then you must also configure the eth3 interface as the device management interface on all the other Junos Space nodes in that fabric.
- When you configure the eth3 interface as the device management interface, the IP addresses of the eth0 and eth3 Ethernet interfaces must be in different subnets.

- Type **Y** if you want to use a different Ethernet interface (eth3) to manage devices.

Configuring device management interface eth3:

```
1> Configure IPv4
2> Configure IPv6
3> Configure Both IPv4 and IPv6
```

R> Redraw Menu

Choice [1-3,R]:

- To configure the IPv4 address of the eth3 interface:

a. Type **1**.

b. Type the IPv4 address for eth3 interface in dotted-decimal notation and press Enter.

```
Please enter new IPv4 address for interface eth3:
192.0.2.25
```

c. Type the new subnet mask of the IPv4 address in dotted-decimal notation and press Enter.

```
Please enter new IPv4 subnet mask for interface eth3:
255.255.0.0
```

d. Type the IPv4 address of the default gateway for the eth3 Ethernet interface in dotted-decimal notation and press Enter.

```
Enter the default IPv4 gateway for this interface:
192.0.2.155
```

- e. Type the IPv4 address of the name server for the eth3 interface and press Enter.

```
Please type the IPv4 nameserver address in dotted decimal notation:
192.0.2.22
```

- To configure the IPv6 address of the eth3 interface:

- a. Type **2**.

- b. Type the IPv6 address with prefix for the eth3 interface.

```
Please enter new IPv6 address with prefix (IPv6 Address/prefix) for
interface eth3:
2001:db8:20:1:192:20:2:50/64
```

- c. Type the IPv6 address of the default gateway for the eth3 interface.

```
Enter the default IPv6 gateway for this interface:
2001:db8:20:1:192:20:2:150
```

- d. Type the IPv6 address of the name server for the eth3 interface and press Enter.

```
Please type the IPv6 nameserver address:
2001:db8:20:1:192:0:2:10
```

- To configure both IPv4 and IPv6 addresses:

- a. Type **3**.

- b. Type the IPv4 address for the eth3 interface in dotted-decimal notation and press Enter.

```
Please enter new IPv4 address for interface eth3:
192.0.2.25
```

- c. Type a subnet mask for the IPv4 address in dotted-decimal notation and press Enter.

```
Please enter new IPv4 subnet mask for interface eth3:
255.255.0.0
```

- d. Type the IPv4 address of the default gateway for the eth3 interface in dotted-decimal notation and press Enter.

```
Enter the default IPv4 gateway for this interface:
192.0.2.155
```

- e. Type the IPv6 address and prefix for the eth3 interface and press Enter.

```
Please enter new IPv6 address with prefix (IPv6 Address/prefix) for
interface eth3:
2001:db8:20:1:192:20:2:50/64
```

NOTE: You must provide an IPv6 address for the name server if you configure an IPv6 address for the eth3 interface.

- f. Type the IPv6 address of the default gateway for the eth3 interface and press Enter.

```
Enter the default IPv6 gateway for this interface:
2001:db8:20:1:192:20:2:150
```

- g. Type the IPv4 address of the name server for the eth3 interface and press Enter.

```
Please type the IPv4 nameserver address in dotted decimal notation:
192.0.2.22
```

- h. Type the IPv6 address of the name server for the eth3 interface and press Enter.

```
Please type the IPv6 nameserver address:
2001:db8:20:1:192:0:2:10
```

- Type **N** if you want to use only the Ethernet interface eth0 to manage devices and the Junos Space Web clients.

12. Specify whether you want to configure the node as a standalone node or you want to add it to an existing cluster.

```
Will this Junos Space system be added to an existing cluster? [y/n]
```

- To add the node to an existing cluster, type **y**.

You are prompted to specify whether you want to configure NAT. Follow the procedure outlined in [“Configuring Access to Junos Space Through a NAT Gateway”](#) on page 62.

- To configure the node as a standalone node, type **n**.

You are prompted to enter the IP address for Web access.

```
Configuring IP address for web GUI:
```

```
1> Configure Both IPv4 and IPv6
```

```
R> Redraw Menu
```

```
Choice [1,R]: 1
```

NOTE: If you configure only an IPv4 address for the eth0 interface, you are provided with an option to configure only the IPv4 address for Web access.

- Type **1** to configure the IPv4 and IPv6 addresses that will be used to access Junos Space Platform through a browser.

NOTE: The IP address for Web access must be in the same subnet as the IP address for the eth0 interface, but must be a different IP address.

- Type the IPv4 address in dotted-decimal notation and press Enter.

```
Please enter IPv4 address for web GUI:
192.0.2.75
```

- Type the IPv6 address and press Enter.

```
Please enter new IPv6 address for web GUI:
2001:db8:0:1:192:0:3:50
```

You are prompted to specify whether you want to configure NAT.

- d. Follow the procedure outlined in [“Configuring Access to Junos Space Through a NAT Gateway” on page 62.](#)

You are then prompted to configure the NTP server.

- e. Specify whether you want to configure the NTP server and time for the Junos Space node:

```
Add NTP Server? [y/n]
```

- To skip configuring the NTP server:

- a. Type **n**.

The current time of the Space node is displayed. You can edit the time or leave it as is.

- b. Press Enter.

- To configure the NTP server:

- a. Type **y** to synchronize the node with an external NTP server and press Enter.

You are prompted to enter the new NTP server.

- b. Enter the IP address or the URI of the NTP server.

```
Please type the new NTP server: device1.example.com
```

On successful addition of the NTP server, a message appears as shown in the following sample:

```
Added device1.example.com
```

You are prompted to enter a display name for the node.

- f. Type a display name for this node and press Enter.

```
Please enter display name for this node: jsnode1
```

This is the name that Junos Space displays for the first node in a Junos Space cluster.

- g. Type the password for cluster maintenance mode and press Enter.

```
Enter password for cluster maintenance mode:
```

NOTE:

- You can choose a password that is at least eight characters long and contains characters from at least three of the following four character classes: uppercase letters, lowercase letters, numbers (0 through 9), and special characters. Ab(3)def, o0*wwrty, and 9Rtsgukj are some examples of valid password for maintenance mode.
- When you configure the other nodes in a cluster (fabric), you are not prompted to enter a maintenance-mode password. The maintenance-mode password that you specify when you configure the first node of the cluster is applicable to all other nodes in that cluster (fabric); in other words, the entire cluster of nodes has the same maintenance-mode password.

You are prompted to retype the password.

```
Re-enter password:
```

- h. Retype the password for cluster maintenance mode and press Enter.

You are prompted to specify whether you want to restore backed up data.

```
Do you want to restore Space backup? [Y/N]:
```

- i. Perform one of the following actions depending on whether you are upgrading Junos Space Platform on the node or configuring a new Junos Space node.
- Type **Y** to restore backed up data if you are upgrading Junos Space Platform.

A message is displayed, warning you to wait till the backed up data is completely restored and all required Junos Space services are started on the node before attempting to access the Web GUI.

The Settings Summary is displayed, as shown in the following example:

```
Settings Summary:
```

```

> IPv4 Change: eth0 is 192.168.26.151 / 255.255.254.0
> Default IPv4 Gateway = 192.168.27.10 on eth0
> IPV6 Change: eth0 is 2001:db8:85a3:0:0:8a2e:c0a9:1b37 / 64
> Default IPv6 Gateway = 2001:db8:85a3:0:0:8a2e:c0a9:1bbd on eth0
> IPv4 DNS add: 192.168.27.2
> DNS add: 2001:db8:85a3:0:0:8a2e:c0a9:1bbd
> Create as first node or standalone
> Web IPv4 address 192.168.26.152
> Web IPv6 address is 2001:db8:85a3:0:0:8a2e:c0a9:1b38/64
> NTP add: device1.example.com
> NAT IPv4 Outbound SSH IP: 192.168.130.2
> NAT IPv4 Outbound SSH Port: 5051
> NAT IPv4 Trap IP: 192.168.130.2
> NAT IPv4 Trap Port: 5052
> NAT IPv6 Outbound SSH IP: 2001:db8:85a3:0:0:130:0:2
> NAT IPv6 Outbound SSH Port: 5053
> NAT IPv6 Trap IP: 2001:db8:85a3:0:0:130:0:2
> NAT IPv6 Trap Port: 5054
> Node display name is "node1"
> Password for Junos Space maintenance mode is set.

A> Apply settings
C> Change settings
Q> Quit and set up later
R> Redraw Menu

Choice [ACQR]:

```

- i. Type **A** and press Enter to apply settings.

You are prompted to specify the location from where you want to restore the backup.

```

1> Remote Server
2> USB
3> Local

M> Return to Main Menu
R> Redraw Menu

Choice [1-3 MR]:

```

- ii. Select one of the following options depending on where the backup file is stored:

- To restore from a remote SCP server:

- i. Type **1** and press Enter.

You are prompted to confirm if you want to proceed with restoring the backup from the remote server.

```
You have selected [ Remote Server ]. Do you want to Continue? [y/N]:
```

- ii. Type **Y** to continue.

You are prompted to enter the IPv4 address of the remote server.

```
Please enter Remote Server IP:
```

- iii. Type the IPv4 address of the remote server and press Enter.

You are prompted to enter the port number of the remote server.

```
Please enter port number for Remote Server <Remote server IP address>:
```

- iv. Enter the port number of the remote server and press Enter.

You are prompted to enter the username to access the remote server.

```
Please enter Remote Server <Remote server IP address> user:
```

- v. Type the username and press Enter.

You are prompted to enter the password of the user.

```
Please enter Remote Server user <Remote server user> password:
```

- vi. Type the password and press Enter.

You are prompted to enter the full path of the directory where the backup file is stored.

```
Enter the path of the directory containing backup files:
```

- vii. Type the full path of the directory and press Enter.

The messages displayed on the console indicate whether the data is restored successfully to the Junos Space node.

- To restore from a USB storage device:

NOTE: Before you restore from a USB storage device, you must ensure that the USB storage device is plugged-in and mounted to the path **/tmp/pendrive**.

- i. Type **2** and press Enter to restore the backup from the USB storage device.

You are prompted to confirm if you want to proceed with the backup from the USB storage device.

```
You have selected [ USB ]. Do you want to Continue? [Y/N]:
```

- ii. Type **Y** to continue.

The messages displayed on the console indicate whether the data is restored successfully to the Junos Space node.

- iii. Unmount the USB storage device by typing the following command:

umount /tmp/pendrive

You can unplug the USB storage device after you unmount it.

- To restore from a local drive:

NOTE: To restore data from a local drive, you must first copy the backup file from the backup location to the Junos Space node.

- i. Type **3** and press Enter.

You are prompted to confirm if you want to proceed with the backup from the local drive.

```
You have selected [ Local ]. Do you want to Continue? [Y/N]:
```

- ii. Type **Y** to continue.

You are prompted to enter the full path of the directory where the back up file is stored.

```
Enter the tar file path to restore from local :
```

iii. Type the full path of the directory and press Enter.

The messages displayed on the console indicate whether the data is restored successfully to the Junos Space node.

When the data is restored successfully, JBoss services are started on the node and you can access the Junos Space Platform UI through a browser by using the virtual IP (VIP) address configured for Web access.

The Junos Space Settings menu is displayed at this point of time after the data is restored and the services restarted.

- Type **N** if you are configuring the first node of a fresh Junos Space Platform 16.1R1 or later installation and not upgrading Junos Space Platform.

A message indicating that you have opted for a fresh installation of Junos Space Platform is displayed. You are prompted to specify whether you want to continue.

```
You have chosen for fresh installation, backup taken from 15.2R2 will not
be restored. Do you want to still proceed with fresh installation?
```

- Perform one of the following actions:
 - Type **Y** to proceed with the fresh installation.
 - Type **N** if you do not want to proceed with the fresh installation.

You are prompted to specify whether you want to restore backed up data.

```
Do you want to Restore Space Backup?
```

- Type **Y** to restore backed up data and go to Step [i](#).
- Type **N** to proceed with the fresh installation.

You are again prompted to confirm whether you want to proceed with a fresh installation. Type **Y** to confirm.

The Settings Summary is displayed, as shown in the following example:

```
Settings Summary:
```

```
> IPv4 Change: eth0 is 192.168.26.151 / 255.255.254.0
```

```

> Default IPv4 Gateway = 192.168.27.10 on eth0
> IPV6 Change: eth0 is 2001:db8:85a3:0:0:8a2e:c0a9:1b37 / 64
> Default IPv6 Gateway = 2001:db8:85a3:0:0:8a2e:c0a9:1bbd on eth0
> IPv4 DNS add: 192.168.27.2
> DNS add: 2001:db8:85a3:0:0:8a2e:c0a9:1bbd
> Create as first node or standalone
> Web IPv4 address 192.168.26.152
> Web IPv6 address is 2001:db8:85a3:0:0:8a2e:c0a9:1b38/64
> NTP add: device1.example.com
> NAT IPv4 Outbound SSH IP: 192.168.130.2
> NAT IPv4 Outbound SSH Port: 5051
> NAT IPv4 Trap IP: 192.168.130.2
> NAT IPv4 Trap Port: 5052
> NAT IPv6 Outbound SSH IP: 2001:db8:85a3:0:0:130:0:2
> NAT IPv6 Outbound SSH Port: 5053
> NAT IPv6 Trap IP: 2001:db8:85a3:0:0:130:0:2
> NAT IPv6 Trap Port: 5054
> Node display name is "node1"
> Password for Junos Space maintenance mode is set.

A> Apply settings
C> Change settings
Q> Quit and set up later
R> Redraw Menu

Choice [ACQR]:A

```

- If the summary information is correct, type **A** to apply the settings.

The Junos Space Settings Menu is displayed, as shown in the following example:

```

Junos Space Settings Menu

1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> Expand VM Drive Size
7> (Debug) run shell

A> Apply Settings
Q> Quit

```

```
R> Redraw Menu

Choice [1-7,QR]:
```

- If the summary information is not correct, type **C** to change the settings.

You are prompted to reenter all the basic configuration information that you have configured up to this point.

13. (Optional) Expand the VM drive size.

NOTE: Before expanding the VM drive size, ensure enough disk space is available on the host for allocation to the partitions of the virtual appliance. If no free space is available on the host for allocation, the **No free disk space** message appears and the Junos Space Settings Menu is displayed.

- Type **6** to expand the VM drive size.

- Enter the admin password.

The following caution appears:

```
-----Caution-----
Expanding Disk drives would stop Jboss and MySQL processes and reboot the
node, all the GUI users would be logged out automatically
Note: This will cause Space Fabric to failover to other node.
```

- Type **y** to continue expanding the drive size or type **n** to return to the Junos Space Settings Menu.

```
Do you want to continue? [y/n]
y
```

If you type **y**, you are prompted to specify the partition that you want to expand.

- Enter the number present against the partition that you want to expand; for example, type **1** to expand the **/** partition or **5** to quit expanding disks and return to the Junos Space Settings Menu.

```
Begin to stop Jboss and MySQL...
Service Jboss and MySQL stopped
```

```
Which partition do you want to expand?
```

```
1) /
2) /var
3) /var/log
4) /tmp
5) Quit
```

```
Select a partition: 1
```

The free space that can be allocated is displayed and you are prompted to enter the space that you want to allocate to the partition.

```
Current disk partition size of / is 22G
Total 4.97G free disk space can be allocated
```

- e. Enter the additional disk space that you want to allocate.

You can enter the disk space in megabytes (M), gigabytes (G), or terabytes (T). Do not add a space between the number and the unit; for example, enter 50M and not 50 M, 10G and not 10 G, and so on.

```
How much additional disk space is to be added(Acceptable suffixes: M|G|T):
1M
```

You are prompted whether you want to expand more drives.

```
Increasing size of LV /dev/jmpvgnocf/lvroot
  Extending logical volume lvroot to 22.59 GB
  Logical volume lvroot successfully resized
Resizing / onto new space, this will take a few minutes
resize4fs 1.41.12 (17-May-2010)
Filesystem at /dev/jmpvgnocf/lvroot is mounted on /; on-line resizing required
old desc_blocks = 2, new_desc_blocks = 2
Performing an on-line resize of /dev/jmpvgnocf/lvroot to 5922816 (4k) blocks.
The filesystem on /dev/jmpvgnocf/lvroot is now 5922816 blocks long.
```

```
4.94G free disk space available
Do you want to expand more disks? [y/N]
```

- f. Type **y** to continue adding disk space or **n** to return to the Junos Space Settings Menu.

When you type **n**, the node is rebooted and the JBoss and MySQL processes that were stopped are resumed. If the VM drive size was expanded on a primary node, the node becomes secondary when it comes up.

14. Type **Q** and press Enter to exit the Junos Space Settings Menu.

The configuration of the Junos Space Virtual Appliance is now complete. It takes approximately 20 to 30 minutes after the configuration for the Junos Space Network Management Platform GUI to be up. You can access the Junos Space Network Management Platform by using a Web browser. Use **super** as the default username and **juniper123** as the password.

NOTE:

- If you have specified that the Junos Space node is the first node in the fabric or a standalone node, you can access Junos Space Network Management Platform by typing the IP address configured for the Web GUI in a browser.
- If you have specified that the Junos Space node is part of an existing cluster (fabric), then you must add the Junos Space node to the Junos Space fabric using the Junos Space Network Management Web GUI. For more information, see the *Adding a Node to an Existing Junos Space Fabric* topic in the *Junos Space Network Management Platform User Guide* (available at <https://www.juniper.net/documentation>).

Configuring Access to Junos Space Through a NAT Gateway

Starting Junos Space Platform Release 16.1R1, you can choose to configure access to Junos Space through a NAT gateway when you are configuring a Junos Space node.

When prompted, specify whether you want to configure access to Junos Space using NAT.

```
Do you want to enable NAT service ? [Y/N]
```

- To configure NAT, type **Y**.

NOTE:

- If you choose to configure NAT, the options that are displayed depend on the IP address or addresses that you have configured for the device management interface. If you have configured eth3 as the device management interface, then the options that are displayed will depend on the IP address or addresses configured for eth3. If eth3 is not configured, the displayed options will depend on the IP address configuration of the eth0 interface.
- If the device management interface is assigned an IPv4 address, you are prompted to enter the IPv4 address for the NAT interfaces. If the device management interface is assigned an IPv6 address, you are prompted to enter the IPv6 address for the NAT interfaces. If the device management interface is assigned an IPv4 address and an IPv6 address, you are prompted to select either IPv4, IPv6, or both for the NAT interfaces.
- If you are adding the node to an existing cluster and eth3 is configured, you are prompted to specify whether you want to configure the trap interface. You must choose to configure the trap interface, if you are adding the node as the standby VIP node. If eth3 is not configured for the node, you are not prompted to configure the trap interface.

You are prompted to configure NAT IP addresses.

```
1> Configure IPv4
2> Configure IPv6
3> Configure IPv4 and IPv6

R> Redraw Menu
Choice [1-3, R]:
```

- To configure the IPv4 address:
 1. Type **1** and press Enter.
 2. Type the IPv4 address of the NAT outbound SSH interface and press Enter.

```
Configuring NAT :

Configuring IPV4 OutboundSSH for NAT:

Please enter the NAT Outbound SSH IP Address
192.168.190.7
```

3. Type the port number of the NAT outbound SSH interface and press Enter.

The port number must be in the range 0-65535.

```
Please enter the NAT Outbound SSH Port Number
4545
```

4. Type the IPv4 address of the NAT trap interface and press Enter.

The IP address must be in the range 1.0.0.1 - 223.255.255.254 excluding 127.x.x.x.

```
Configuring IPV4 Trap for NAT:

Please enter the NAT Trap IP Address
192.168.27.1
```

5. Type the port number of the NAT trap interface and press Enter.

```
Please enter the NAT Trap Port Number
4584
```

- To configure the IPv6 address:

1. Type 2 and press Enter.
2. Type the IPv6 address of the NAT outbound SSH interface and press Enter.

```
Configuring NAT :

Configuring IPV6 OutboundSSH for NAT:

Please enter the NAT Outbound SSH IP Address
2001:db8:85a3::8a2e:130:0:2
```

3. Type the port number of the NAT outbound SSH interface and press Enter.

The port number must be in the range 0-65535.

```
Please enter the NAT Outbound SSH Port Number
5054
```

4. Type the IPv6 address of the NAT trap interface and press Enter.

The IP address must be in the range 1.0.0.1 - 223.255.255.254 excluding 127.x.x.x

Configuring IPV6 Trap for NAT:

Please enter the NAT Trap IP Address

2001:db8:85a3::8a2e:130:0:2

5. Type the port number of the NAT trap interface and press Enter.

Please enter the NAT Trap Port Number

5054

- To configure IPv4 and IPv6:

1. Type **3** and press Enter.

2. Type the IPv4 address of the NAT outbound SSH interface and press Enter.

The IP address must be in the range 1.0.0.1 - 223.255.255.254 excluding 127.x.x.x.

Configuring IPV4 OutboundSSH for NAT:

Please enter the NAT Outbound SSH IP Address

192.168.190.7

3. Type the port number of the NAT outbound SSH interface and press Enter.

The port number must be in the range 0-65535.

Please enter the NAT Outbound SSH Port Number

4545

4. Type the IPv4 address of the NAT trap interface and press Enter.

The IP address must be in the range 1.0.0.1 - 223.255.255.254 excluding 127.x.x.x.

Configuring IPV4 Trap for NAT:

Please enter the NAT Trap IP Address

192.168.27.1

5. Type the port number of the NAT trap interface and press Enter.

The port number must be in the range 0-65535.

```
Please enter the NAT Trap Port Number
4584
```

6. Type the IPv6 address of the NAT outbound SSH interface and press Enter.

```
Configuring IPV6 OutboundSSH for NAT:

Please enter the NAT Outbound SSH IP Address
2001:db8:85a3::8a2e:130:0:2
```

7. Type the port number of the NAT outbound SSH interface and press Enter.

The port number must be in the range 0-65535.

```
Please enter the NAT Outbound SSH Port Number
7075
```

8. Type the IPv6 address of the NAT trap interface and press Enter.

The IP address must be in the range 1.0.0.1 - 223.255.255.254 excluding 127.x.x.x.

```
Configuring IPV6 Trap for NAT:

Please enter the NAT Trap IP Address
2001:db8:85a3::8a2e:130:0:2
```

9. Type the port number of the NAT trap interface and press Enter.

The port number must be in the range 0-65535.

```
Please enter the NAT Trap Port Number
7076
```

- If you do not want to configure NAT, type **N** and press Enter.

If you are configuring a standalone node, you are prompted to configure the NTP server. Go to Step [e](#).

If you are configuring a node to be added to an existing cluster, the Settings Summary is displayed, as shown in the following example:

```
Settings Summary

> IPv4 Change: eth0 is 192.168.26.151 / 255.255.254.0
> Default IPv4 Gateway = 192.168.27.10 on eth0
> IPV6 Change: eth0 is 2001:db8:30:0:0:26:0:97 / 120
> Default IPv6 Gateway = 2001:db8:30:0:0:26:0:95 on eth0
> IPv4 DNS add: 192.168.27.2
> DNS add: 2001:db8:30:0:0:26:0:97
> IPv4 Change: eth3 is 192.168.130.2 / 255.255.254.0
> eth3 IPv4 Gateway: 192.168.130.5
> IPV6 Change: eth3 is 2001:db8:35:0:0:130:0:97 / 120
> eth3 IPv6 Gateway: 2001:db8:35:0:0:130:0:95
> NAT IPv4 Outbound SSH IP: 192.168.26.213
> NAT IPv4 Outbound SSH Port: 5051
> NAT IPv6 Outbound SSH IP: 2001:db8:85a3::8a2e:130:0:2
> NAT IPv6 Outbound SSH Port: 5053
> Node to be added to existing cluster

A> Apply settings
C> Change settings
Q> Quit and set up later
R> Redraw Menu

Choice [ACQR]:
```

- If the summary information is correct, type **A** to apply the settings.

The Junos Space Settings Menu is displayed, as shown in the following example:

```
Junos Space Settings Menu

1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> Expand VM Drive Size
7> (Debug) run shell
```

```

A> Apply Settings
Q> Quit
R> Redraw Menu

Choice [1-7,QR]:

```

- If the summary information is not correct, type **C** to change the settings.

You are prompted to reenter all the basic configuration information that you have configured up to this point.

- To quit the configuration without applying the settings, type **Q**.

The Junos Space Settings Menu is displayed.



CAUTION: If you quit the configuration without applying the settings, then all the settings are discarded.

Configuring the eth1 Ethernet Interface

You use the eth1 Ethernet interface as the administrative interface for a Junos Space node. Configure the eth1 interface after the Junos Space node reboots after completing the basic configuration.

NOTE:

- The eth1 interface must be configured separately for each node in a multinode fabric.
- If you configure the eth1 interface, SSH is disabled on the eth0 and the eth3 interfaces. You can then access the CLI of the Junos Space virtual appliance only through the eth1 interface.

To configure the eth1 interface:

1. On the Junos Space Settings Menu, type **7** to access the shell.

You are prompted to enter your password.

2. Type your password and press Enter.

The shell prompt appears.

3. At the shell prompt, type **jmp_config** and press Enter.

You are prompted to enter the IP address of the eth1 interface.

4. Type the IP address of the eth1 interface in dotted-decimal notation and press Enter.

The IP address can be in the same subnet as the virtual IP (VIP) address or in a different subnet. If the IP address is not in the same subnet as the VIP address, you are prompted to enter the subnet mask and then the default gateway for the eth1 interface.

5. (Optional) Type the subnet mask for the eth1 interface in dotted-decimal notation and press Enter.

6. (Optional) Type the default gateway in dotted-decimal notation and press Enter.

The eth1 interface is configured.

7. To verify that the eth1 address is configured, run the **ifconfig eth1** command and check that the IP address displayed for eth1 is the same as the one that you configured.

You can now access the Junos Space node through the eth1 interface to perform administrative tasks.

To troubleshoot issues in configuring the eth1 interface, refer to the **/var/log/changeEth1.log** file.

Release History Table

Release	Description
16.1R1	From Junos Space Network Management Platform Release 16.1R1 onward, you can configure access to Junos Space through a Network Address Translation (NAT) gateway.
16.1R1	Starting Junos Space Platform Release 16.1R1, you can choose to configure access to Junos Space through a NAT gateway when you are configuring a Junos Space node.

RELATED DOCUMENTATION

Logging In to Junos Space

[Ethernet Interfaces in a Junos Space Virtual Appliance Overview | 13](#)

[Adding a Node to an Existing Junos Space Fabric | 141](#)

[Junos Space Virtual Appliance Deployment Overview | 19](#)

Configuring a Junos Space Virtual Appliance as a Standalone or Primary FMPM Node

IN THIS SECTION

- [Configuring the Junos Space Virtual Appliance as the Primary FMPM Node | 71](#)

You can configure a Junos Space Virtual Appliance as a Junos Space node or as a specialized network monitoring node used for fault monitoring and performance monitoring (FMPM). An FMPM node can be configured as a standalone or primary FMPM node, or as a secondary or backup FMPM node. The first FMPM node that you configure is always the standalone or primary node; this node performs fault and performance monitoring of the devices and nodes, and any events or alarms are stored in a PostgreSQL database on this node. This topic explains how you can configure a Junos Space Virtual Appliance as a primary FMPM node.

NOTE: You must have at least one Junos Space node already configured to add an FMPM node in a cluster.

To configure a Junos Space Virtual Appliance as a standalone or primary FMPM node, you must configure basic network and system settings to make the node accessible on the network.

NOTE:

- From Junos Space Network Management Platform Release 14.1R2 onward, you can configure Junos Space Ethernet interfaces with only IPv4 addresses, or both IPv4 and IPv6 addresses.
- From Junos Space Network Management Platform Release 16.1R1 onward, you can configure access to Junos Space through a Network Address Translation (NAT) gateway.

Before you begin, do the following:

- Ensure that 100 GB free disk space is available before configuring a node as an FMPM node.
- Before you begin, ensure that you have the following information available:
 - IPv4 address and subnet mask for the eth0 Ethernet interface
 - (Optional) IPv6 address and prefix for the eth0 Ethernet interface

- IPv4 address of the default gateway
- (Optional) IPv6 address of the default gateway
- IPv4 address of the name server
- (Optional) IPv6 address of the name server
- Virtual IP (VIP) address of the FMPM nodes in IPv4 and IPv6 formats

The VIP address is used for communications between Junos Space nodes and FMPM nodes. This IP address must be in the same subnet as the IP address assigned to the eth0 Ethernet interface, and the VIP address must be different from the VIP address used to access the Web GUI.

- IPv4 address or URL of NTP source to synchronize time
- (Optional) IPv4 address of the eth1 Ethernet interface.

If the IP address of the eth1 interface is not in the same subnet as the VIP address, ensure that you have the subnet mask and the default gateway for the eth1 interface.

- (Optional) IPv4 address for the NAT trap
- (Optional) IPv6 address for the NAT trap
- (Optional) Port number for the NAT trap

Before you begin, ensure that you have the following information available:

This topic discusses the following tasks:

Configuring the Junos Space Virtual Appliance as the Primary FMPM Node

You can configure a Junos Space Virtual Appliance as an FMPM node.

To configure the virtual appliance as the first or primary FMPM node:

1. Using a virtual machine client (such as VMware vSphere Client or Virtual Machine Manager [VMM]), log in and power on the Junos Space Virtual Appliance.
2. Access the console on the virtual machine client to view the Junos Space login prompt.
3. At the Junos Space login prompt, type **admin** as your default login name and press Enter.
4. Type **abc123** as your default password and press Enter.
Junos Space prompts you to change your default password.
5. Type the default password again and press Enter.

6. Type the new password and press Enter.

NOTE: You can choose a password that is at least eight characters long and contains characters from at least three of the following four character classes: uppercase letters, lowercase letters, numbers (0 through 9), and special characters.

However, if a password satisfies the preceding criteria but contains only a single uppercase letter at the beginning or only a single number at the end, then that password is considered invalid. For example, Abcdwip9, Qc9rdiwt, and bRfjvin9 are invalid passwords, but AAbcdwip99, Qc9rdiwtQ, and bRfjvin99 are valid passwords.

Alternatively, instead of using a string of characters, you can choose a passphrase that is between 16 and 40 characters long and contains at least three dictionary words separated by at least one special character. For example, big#three;fork (14 characters long) and circlefaceglass (no special characters) are invalid passphrases, but @big#three;fork& and circle;face;glass are valid passphrases.

Passwords and passphrases are case-sensitive.

7. Retype your new password.

If the password is changed successfully, the message **passwd: all authentication tokens updated successfully.** is displayed.

8. Type **F** to configure the virtual appliance as a standalone or primary FMPM node and press Enter when prompted Choose the type of node to be installed.

```
Choose the type of node to be installed [S/F] F
```

9. Configure the IP address of the eth0 Ethernet interface.

This IP address will be used as the IP address of the FMPM node.

```
Configuring Eth0 :

1> Configure IPv4
2> Configure Both IPv4 and IPv6

R> Redraw Menu

Choice [1-2,R]:
```


- To configure the IPv4 address of the eth0 interface:
 - a. Type 1.
 - b. Type the IPv4 address for the eth0 interface in dotted-decimal notation and press Enter.

```
Please enter new IPv4 address for interface eth0:  
192.0.2.25
```

NOTE: All nodes that you configure in a cluster (fabric) must be in the same subnet.

- c. Type the new subnet mask for the IPv4 address and press Enter.

```
Please enter new IPv4 subnet mask for interface eth0:  
255.255.0.0
```

- d. Type the IP address of the default gateway for the eth0 Ethernet interface in dotted-decimal notation and press Enter.

```
Enter the default IPv4 gateway as a dotted-decimal IP address:  
192.0.2.155
```

- To configure both IPv4 and IPv6 addresses:
 - a. Type 2.
 - b. Type the IPv4 address for the eth0 interface in dotted-decimal notation and press Enter.

```
Please enter new IPv4 address for interface eth0  
192.0.2.25
```

- c. Type a subnet mask for the eth0 interface in dotted-decimal notation and press Enter.

```
Please enter new IPv4 subnet mask for interface eth0:  
255.255.0.0
```

- d. Type the IPv4 address of the default gateway for the eth0 interface in dotted-decimal notation and press Enter.

```
Enter the default IPv4 gateway as a dotted-decimal IP address:
192.0.2.155
```

- e. Type the IPv6 address and prefix for the eth0 interface and press Enter.

```
Please enter new IPv6 address with prefix (IPv6 Address/prefix) for interface
eth0:
2001:db8:10:1:192:10:2:50/64
```

- f. Type the IPv6 address of the default gateway for the eth0 interface and press Enter.

```
Enter the IPv6 gateway:
2001:db8:0:1:192:10:2:150
```

10. Type the IPv4 address of the name server and press Enter.

```
Please type the IPv4 nameserver address in dotted decimal notation:
192.0.2.15
```

11. Type the IPv6 address of the name server and press Enter.

```
Please type the IPv6 nameserver address:
2001:db8:0:1:192:10:2:10
```

12. Type **P** when prompted Choose the role for this FMPM specialized node [P/B].

The FMPM node can be configured as follows:

- (P)rimary - Standalone or first FMPM node in an FMPM high availability pair
- (B)ackup - Backup FMPM node in an FMPM high availability pair

Choosing P installs the node as a standalone FMPM node or the primary node in an FMPM HA setup. This node performs fault and performance monitoring of the devices and nodes, and any events or alarms is stored in a PostgreSQL database on this node.

13. Configure the IP address for the FMPM service.

This IP address is the VIP address of the FMPM nodes and is used for communication between the Junos Space nodes and the FMPM nodes.

NOTE: The FMPM service IP address and the FMPM node IP address should be in the same subnet.

Configuring IP address for FMPM service:

1> Configure Both IPv4 and IPv6

R> Redraw Menu

Choice [1,R]:

NOTE: If you configure only an IPv4 address for the eth0 interface, you are provided with an option to configure only the IPv4 address for the FMPM service.

- a. Type **1** to configure the IPv4 and IPv6 addresses for the FMPM service.
- b. Type the IPv4 address for the FMPM service and press Enter.

Please enter IPv4 address for FMPM service:
192.0.2.75

- c. Type the IPv6 address for the FMPM service and press Enter.

Please enter new IPv6 address for FMPM service
2001:db8:0:1:192:10:3:50

You are prompted to specify whether you want to configure NAT.

14. Specify whether you want to configure access to Junos Space using NAT.

Do you want to enable NAT service ? [Y/N]

- To configure NAT, type Y.

NOTE: If you choose to configure NAT, the options that are displayed depend on the IP address or addresses that you have configured for the eth0 interface. If the eth0 interface is assigned an IPv4 address, you are prompted to enter the IPv4 address for the NAT trap interface. If the eth0 interface is assigned an IPv4 address and an IPv6 address, you are prompted to configure either an IPv4 address, an IPv6 address, or both IPv4 and IPv6 addresses for the NAT trap interface.

You are prompted to configure NAT IP addresses.

```
1> Configure IPv4
2> Configure IPv6
3> Configure IPv4 and IPv6

R> Redraw Menu
Choice [1-2, R]:
```

- To configure the IPv4 address:
 - a. Type **1** and press Enter.
 - b. Type the IPv4 address of the NAT trap interface and press Enter.

The IP address must be in the range 1.0.0.1 - 223.255.255.254 excluding 127.x.x.x.

```
Configuring IPV4 Trap for NAT:

Please enter the NAT Trap IP Address
192.168.27.1
```

- c. Type the port number of the NAT trap interface and press Enter.

The port number must be in the range 0-65535.

```
Please enter the NAT Trap Port Number
4584
```

- To configure the IPv6 address:
 - a. Type **2** and press Enter.

- b. Type the IPv6 address of the NAT trap interface and press Enter.

```
Configuring IPV6 Trap for NAT:

Please enter the NAT Trap IP Address
2001:db8:85a3::8a2e:130:0:5
```

- c. Type the port number of the NAT trap interface and press Enter.

The port number must be in the range 0-65535.

```
Please enter the NAT Trap Port Number
5055
```

- To configure IPv4 and IPv6:

- a. Type **3** and press Enter.

- b. Type the IPv4 address of the NAT trap interface and press Enter.

The IP address must be in the range 1.0.0.1 - 223.255.255.254 excluding 127.x.x.x.

```
Configuring IPV4 Trap for NAT:

Please enter the NAT Trap IP Address
192.168.27.1
```

- c. Type the port number of the NAT trap interface and press Enter.

The port number must be in the range 0-65535.

```
Please enter the NAT Trap Port Number
4584
```

- d. Type the IPv6 address of the NAT trap interface and press Enter.

```
Configuring IPV6 Trap for NAT:

Please enter the NAT Trap IP Address
2001:db8:85a3::8a2e:130:0:5
```

- e. Type the port number of the NAT trap interface and press Enter.

The port number must be in the range 0-65535.

```
Please enter the NAT Trap Port Number
5055
```

- If you do not want to configure NAT, type **N** and press Enter.

You are prompted to specify whether you want to add an NTP server.

15. Add an NTP server to synchronize the node with an external NTP source or specify the current time for the FMPM node.

- To add an NTP server, type **y**, enter the hostname of the NTP server when prompted, and press Enter.
- To specify the current time (UTC), type **n**, enter the time, and press Enter.

The settings summary is displayed, as shown in the following example:

```
Settings Summary:

> IPv4 Change: eth0 is 192.168.26.151 / 255.255.254.0
> Default IPv4 Gateway = 192.168.27.10 on eth0
> IPV6 Change: eth0 is 2001:db8:85a3:0:0:8a2e:c0a9:1b37 / 64
> Default IPv6 Gateway = 2001:db8:85a3:0:0:8a2e:c0a9:1bbd on eth0
> IPv4 DNS add: 192.168.27.2
> DNS add: 2001:db8:85a3:0:0:8a2e:c0a9:1bbd
> Create as first node or standalone
> FMPM service IPv4 address is 192.68.26.153
> Web IPv6 address is 2001:db8:85a3:0:0:8a2e:c0a9:1b38/64
> NTP add: device1.example.com
> NAT IPv4 Trap IP: 192.168.26.213
> NAT IPv4 Trap Port: 5056
> NAT IPv6 Trap IP: 2001:db8:85a3::8a2e:130:0:5

> NAT IPv6 Trap Port: 5058
> Node display name will be set when it is added.
> This node will be the primary FMPM specialized node.

A> Apply settings
C> Change settings
Q> Quit and set up later
R> Redraw Menu
```

```
Choice [ACQR]:
```

16. Confirm that the information in the Settings Summary is correct:

- If all summary information is correct, enter **A** to apply the settings.
- If any summary information is incorrect, enter **C** to change the settings.

If you enter C, you are prompted to retype all the basic configuration information that you have configured up to this point.

17. Expand the VM drive size.

Expand the /var partition by 120 GB.

NOTE: Before expanding the VM drive size for an FMPM node, ensure that enough disk space is available on the host for allocation to the partitions. If no free space is available for allocation, the **No free disk space** message appears and the Junos Space Settings Menu is displayed.

The minimum disk space required for the /var partition is 120 GB.

- Type **6** to expand the VM drive size.
- Enter the admin password.

NOTE: No caution is displayed for node reboot while expanding the drive size for an FMPM node. However, the FMPM node is rebooted after the drive size is expanded.

- Type **y** to continue expanding the drive size or type **n** to return to the Junos Space Settings Menu.

```
Do you want to continue? [y/n]
y
```

If you type **y**, you are prompted to specify the partition that you want to expand.

- Enter the number present against the partition that you want to expand; for example, type **2** to expand the /var partition or **5** to quit expanding disks and return to the Junos Space Settings Menu.

The free space that can be allocated is displayed and you are prompted to enter the space that you want to allocate to the partition.

```
Begin to stop Jboss ...
Service Jboss stopped

Which partition do you want to expand?

1) /
2) /var
3) /var/log
4) /tmp
5) Quit
Select a partition: 1
```

- e. Type the additional disk space that you want to allocate and press Enter.

You can enter the disk space in megabytes (M), gigabytes (G), or terabytes (T). Do not add a space between the number and the unit; for example, 50M and not 50 M, 10G and not 10 G, and so on.

```
Current disk partition size of / is 22G
Total 4.97G free disk space can be allocated

How much additional disk space is to be added(Acceptable suffixes: M|G|T):
1M
```

You are prompted whether you want to expand more drives.

```
Increasing size of LV /dev/jmpvgnocf/lvroot
  Extending logical volume lvroot to 22.59 GB
  Logical volume lvroot successfully resized
Resizing / onto new space, this will take a few minutes
resize4fs 1.41.12 (17-May-2010)
Filesystem at /dev/jmpvgnocf/lvroot is mounted on /; on-line resizing required
old desc_blocks = 2, new_desc_blocks = 2
Performing an on-line resize of /dev/jmpvgnocf/lvroot to 5922816 (4k) blocks.
The filesystem on /dev/jmpvgnocf/lvroot is now 5922816 blocks long.

4.94G free disk space available
```



```
Do you want to expand more disks? [y/N]
N
```

- f. Type **y** to continue adding disk space or **N** to return to the Junos Space Settings Menu.

When you type **N**, the node is rebooted and the opennms process that was stopped is resumed. If the VM drive size was expanded on a primary node, the node becomes secondary when it comes up.

18. Type **Q** to exit the Junos Space Settings Menu.

The FMPM node is ready to be added to the space cluster. See [“Adding a Node to an Existing Junos Space Fabric” on page 141](#) for information about adding a node to the Junos Space cluster.

RELATED DOCUMENTATION

[Junos Space Virtual Appliance Deployment Overview | 19](#)

[Adding a Node to an Existing Junos Space Fabric | 141](#)

[Ethernet Interfaces in a Junos Space Virtual Appliance Overview | 13](#)

Configuring a Junos Space Virtual Appliance as a Backup or Secondary FMPM Node for High Availability

IN THIS SECTION

- [Configuring a Junos Space Virtual Appliance as a Backup or Secondary FMPM Node | 83](#)

You can configure a Junos Space Virtual Appliance as a Junos Space node or as a specialized network monitoring node used for fault monitoring and performance monitoring (FMPM).

An FMPM node can be configured as a standalone or primary FMPM node, or as a secondary or backup FMPM node. The first FMPM node that you configure is always the standalone or primary node; this node performs fault and performance monitoring of the devices and nodes, and any events or alarms are stored in a PostgreSQL database on this node. The second FMPM node that you configure is the backup or

secondary FMPM node. The PostgreSQL database containing the fault and performance monitoring data is replicated from the primary FMPM node to the secondary FMPM node. When the primary node is down or being rebooted, the secondary node automatically assumes charge.

A primary and a secondary FMPM node are referred to as a cluster or a team; therefore, an FMPM team can consist of a maximum of two nodes.

NOTE: You must have at least one Junos Space node, and a primary FMPM node, before you configure a secondary FMPM node.

To configure a Junos Space Virtual Appliance as a backup or secondary FMPM node, you must configure basic network and system settings to make the node accessible on the network.

NOTE: From Junos Space Network Management Platform Release 14.1R2 onward, you can configure Junos Space Ethernet interfaces with only IPv4 addresses, or both IPv4 and IPv6 addresses.

Before you begin, do the following:

- Ensure that 100 GB free disk space is available before configuring a node as an FMPM node.
- Before you begin, ensure that you have the following information available:
 - IPv4 address and subnet mask for the eth0 Ethernet interface
 - (Optional) IPv6 address and prefix for the eth0 Ethernet interface
 - IPv4 address of the default gateway
 - (Optional) IPv6 address of the default gateway
 - IPv4 address of the name server
 - (Optional) IPv6 address of the name server
 - Virtual IP (VIP) address of the FMPM nodes in IPv4 and IPv6 formats

The VIP address is used for communications between Junos Space nodes and FMPM nodes. This IP address must be in the same subnet as the IP address assigned to the eth0 Ethernet interface, and the VIP address must be different from the VIP address used to access the Web GUI.

- IPv4 address or URL of NTP source to synchronize time
- (Optional) IPv4 address of the eth1 Ethernet interface.

If the IP address of the eth1 interface is not in the same subnet as the VIP address, ensure that you have the subnet mask and the default gateway for the eth1 interface.

- (Optional) IPv4 address for the NAT trap
- (Optional) IPv6 address for the NAT trap
- (Optional) Port number for the NAT trap

Before you begin, ensure that you have the following information available:

This topic discusses the following tasks:

Configuring a Junos Space Virtual Appliance as a Backup or Secondary FMPM Node

You can configure a Junos Space Virtual Appliance as a backup FMPM node.

To add a secondary or backup FMPM node to the Junos Space cluster:

1. Using a virtual machine client (such as VMware vSphere Client or Virtual Machine Manager [VMM]), log in and power on the Junos Space Virtual Appliance.
2. Access the console on the virtual machine client to view the Junos Space login prompt.
3. At the Junos Space login prompt, type **admin** as your default login name and press Enter.
4. Type **abc123** as your default password and press Enter.
Junos Space prompts you to change your default password.
5. Type the default password again and press Enter.
6. Type the new password and press Enter.

NOTE: You can choose a password that is at least eight characters long and contains characters from at least three of the following four character classes: uppercase letters, lowercase letters, numbers (0 through 9), and special characters.

However, if a password satisfies the preceding criteria but contains only a single uppercase letter at the beginning or only a single number at the end, then that password is considered invalid. For example, Abcdwip9, Qc9rdiwt, and bRfjvin9 are invalid passwords, but AAbcdwip99, Qc9rdiwtQ, and bRfjvin99 are valid passwords.

Alternatively, instead of using a string of characters, you can choose a passphrase that is between 16 and 40 characters long and contains at least three dictionary words separated by at least one special character. For example, big#three;fork (14 characters long) and circlefaceglass (no special characters) are invalid passphrases, but @big#three;fork& and circle;face;glass are valid passphrases.

Passwords and passphrases are case-sensitive.

7. Retype your new password.

If the password is changed successfully, the message **passwd: all authentication tokens updated successfully.** is displayed.

8. Type **F** to configure the virtual appliance as a standalone or primary FMPM node and press Enter when prompted Choose the type of node to be installed.

```
Choose the type of node to be installed [S/F] F
```

9. Configure the IP address of the eth0 Ethernet interface.

This IP address is used as the IP address of the FMPM node.

```
Configuring Eth0 :

1> Configure IPv4
2> Configure Both IPv4 and IPv6

R> Redraw Menu

Choice [1-2,R]:
```

- To configure the IPv4 address of the eth0 interface:
 - a. Type 1.
 - b. Type the IPv4 address for the eth0 interface in dotted-decimal notation and press Enter.

```
Please enter new IPv4 address for interface eth0:  
192.0.2.53
```

NOTE: All nodes that you configure in a cluster (fabric) must be in the same subnet.

- c. Type the new subnet mask for the IPv4 address and press Enter.

```
Please enter new IPv4 subnet mask for interface eth0:  
255.255.0.0
```

- d. Type the IP address of the default gateway for the eth0 Ethernet interface in dotted-decimal notation and press Enter.

```
Enter the default IPv4 gateway as a dotted-decimal IP address:  
192.0.2.155
```

- To configure both IPv4 and IPv6 addresses:
 - a. Type 2.
 - b. Type the IPv4 address for the eth0 interface in dotted-decimal notation and press Enter.

```
Please enter new IPv4 address for interface eth0  
192.0.2.53
```

- c. Type a subnet mask for the eth0 interface in dotted-decimal notation and press Enter.

```
Please enter new IPv4 subnet mask for interface eth0:  
255.255.0.0
```

- d. Type the IPv4 address of the default gateway for the eth0 interface in dotted-decimal notation and press Enter.

```
Enter the default IPv4 gateway as a dotted-decimal IP address:
192.0.2.155
```

- e. Type the IPv6 address and prefix for the eth0 interface and press Enter.

```
Please enter new IPv6 address with prefix (IPv6 Address/prefix) for interface
eth0:
2001:db8:0:1:192:10:2:51/64
```

- f. Type the IPv6 address of the default gateway for the eth0 interface and press Enter.

```
Enter the IPv6 gateway:
2001:db8:0:1:192:10:2:150
```

10. Type the IPv4 address of the name server and press Enter.

```
Please type the IPv4 nameserver address in dotted decimal notation:
192.0.2.15
```

11. Type the IPv6 address of the name server and press Enter.

```
Please type the IPv6 nameserver address:
2001:db8:0:1:192:10:2:10
```

12. Enter **B** when prompted Choose the role for this FMPM specialized node [P/B].

Choosing B installs the node as the secondary or backup node in an FMPM HA setup. The PostgreSQL database containing the fault and performance monitoring data is replicated from the primary node to this node. When the primary node is down or being rebooted, the backup node automatically assumes charge.

The settings summary is displayed, as shown in the following example:

```
1> IP Change: eth0 is 10.205.56.136 / 255.255.0.0
2> Default Gateway = 10.205.255.254 on eth0
3> DNS add: 10.209.194.14
4> This node will be the backup FMPM specialized node.
```

```

1> IPv4 Change: eth0 is 192.0.2.53 / 255.255.0.0
2> Default IPv4 Gateway = 192.0.2.155 on eth0
3> IPV6 Change: eth0 is 2001:db8:0:1:192:10:2:51 / 64
4> Default IPv6 Gateway = 2001:db8:0:1:192:10:2:150 on eth0
5> IPv4 DNS add: 192.0.2.15
6> DNS add: 2001:db8:0:1:192:10:2:10
8> This node will be the backup FMPM specialized node.

A> Apply settings
C> Change settings
Q> Quit and set up later
R> Redraw Menu

Choice [ACQR]:

```

13. Confirm that the information in the settings summary is correct:

- If all summary information is correct, enter **A** to apply the settings
- If any summary information is incorrect, enter **C** to change the settings

If you enter C, you are prompted to reenter all the basic configuration information that you have configured up to this point.

14. Expand the VM drive size.

Expand the /var partition by 120 GB.

- Type **6** to expand the VM drive size.

NOTE: Before expanding the VM drive size, ensure free disk space is available for allocation to the partitions. For information about adding disk resources, refer to [“Deploying a Junos Space Virtual Appliance on a VMware ESXi Server”](#) on page 23.

The minimum disk space required for the /var partition is 120 GB.

- Enter the administrator password.

NOTE: No caution is displayed for node reboot while expanding the drive size for an FMPM node. However, the FMPM node is rebooted after the drive size is expanded.

- c. Type **y** to continue expanding the drive size or type **n** to return to the Junos Space Settings Menu.

```
Do you want to continue? [y/n]
y
```

If you type **y**, you are prompted to specify the partition that you want to expand.

- d. Enter the number present against the partition that you want to expand; for example, type **2** to expand the **/var** partition or **5** to quit expanding disks and return to the Junos Space Settings Menu.

The free space that can be allocated is displayed and you are prompted to enter the space that you want to allocate to the partition.

```
Begin to stop Jboss ...
Service Jboss stopped

Which partition do you want to expand?

1) /
2) /var
3) /var/log
4) /tmp
5) Quit
Select a partition: 1
```

- e. Enter the additional disk space that you want to allocate.

You can enter the disk space in megabytes (M), gigabytes (G), or terabytes (T). Do not add a space between the number and the unit; for example, 50M and not 50 M, 10G and not 10 G, and so on.

```
Current disk partition size of / is 22G
Total 4.97G free disk space can be allocated

How much additional disk space is to be added(Acceptable suffixes: M|G|T):
1M
```

You are prompted whether you want to expand more drives.

```
Increasing size of LV /dev/jmpvgnocf/lvroot
Extending logical volume lvroot to 22.59 GB
Logical volume lvroot successfully resized
```



```
Resizing / onto new space, this will take a few minutes
resize4fs 1.41.12 (17-May-2010)
Filesystem at /dev/jmpvgnocf/lvroot is mounted on /; on-line resizing required
old desc_blocks = 2, new_desc_blocks = 2
Performing an on-line resize of /dev/jmpvgnocf/lvroot to 5922816 (4k) blocks.
The filesystem on /dev/jmpvgnocf/lvroot is now 5922816 blocks long.

4.94G free disk space available
Do you want to expand more disks? [y/N]
N
```

- f. Type **y** to continue adding disk space or **n** to return to the Junos Space Settings Menu.

When you type **n**, the node is rebooted and the opennms process that was stopped is resumed. If the VM drive size was expanded on a primary node, the node becomes secondary when it comes up.

15. Type **Q** to exit the Junos Space Settings Menu.

The FMPM node is ready to be added to the Junos Space cluster. See [“Adding a Node to an Existing Junos Space Fabric” on page 141](#) for information about adding a node to the Junos Space cluster.

RELATED DOCUMENTATION

[Ethernet Interfaces in a Junos Space Virtual Appliance Overview | 13](#)

[Junos Space Virtual Appliance Deployment Overview | 19](#)

[Adding a Node to an Existing Junos Space Fabric | 141](#)

Changing the Network and System Settings of a Junos Space Virtual Appliance

You can change some basic options that you configured when you first installed and set up your Junos Space Virtual Appliance. You can also change the default system time and retrieve system log files from your Junos Space Virtual Appliance.

Each time you log in from the Junos Space system console, the Junos Space Settings Menu is displayed as follows:

```
1> Change Password
2> Change Network Settings
3> Change Time Options
4> Retrieve Logs
5> Security
6> Expand VM Drive Size
7> (Debug) run shell

A> Apply changes
Q> Quit
R> Redraw Menu

Choice [1-7,AQR]:
```

Follow the system prompts from the menu to set or modify menu options. Password changes take effect immediately. Other configuration changes you make do not take effect until you apply the changes.

NOTE: An openNMS user does not have permission to modify the Junos Space Settings.

To change a Junos Space Virtual Appliance configuration, you must be a user with administrative privileges and already logged in to the Junos Space Virtual Appliance. You can perform the following tasks from the Junos Space Settings Menu:

- [Changing the admin User Password of a Junos Space Virtual Appliance | 90](#)
- [Changing the Network Settings of a Junos Space Virtual Appliance | 92](#)
- [Changing Time Options of a Junos Space Virtual Appliance | 126](#)
- [Retrieving System Log Files from a Junos Space Virtual Appliance | 130](#)
- [Expanding the Drive Size of a Junos Space Virtual Appliance | 132](#)
- [Setting Security Options on a Junos Space Virtual Appliance | 135](#)
- [Running Shell in a Junos Space Virtual Appliance | 138](#)

Changing the admin User Password of a Junos Space Virtual Appliance

You can change the admin user password used to log in to the Junos Space Network Management Platform.

To change the administrator password:

1. At the Junos Space Settings Menu prompt, type **1**.

The Change Password menu appears:

```
Change Password:
1> Change password for user admin

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1,AMR]:
```

2. Type **1** at the command prompt.

You are prompted for confirmation.

```
Password changes will take effect immediately
Change password for user admin? [y/N]
```

3. Type **y**.

You are prompted for the current administrator password.

```
Changing password for user admin.
Changing password for admin
(current) UNIX password:
```

4. Enter the current administrator password.

You are prompted to enter the new administrator password.

```
New UNIX password:
```

5. Enter the new password.

You can choose a password that is at least eight characters long and contains characters from at least three of the following four character classes: uppercase letters, lowercase letters, numbers (0 through 9), and special characters.

However, if a password satisfies the preceding criteria but contains only a single uppercase letter at the beginning or only a single number at the end, then that password is considered invalid. For example,

Abcdwip9, Qc9rdiwt, and bRfjvin9 are invalid passwords, but AAbcdwip99, Qc9rdiwtQ, and bRfjvin99 are valid passwords.

Alternatively, instead of using a string of characters, you can choose a passphrase that is between 16 and 40 characters long and contains at least three dictionary words separated by at least one special character. For example, big#three;fork (14 characters long) and circlefaceglass (no special characters) are invalid passphrases, but @big#three;fork& and circle;face;glass are valid passphrases.

Passwords and passphrases are case-sensitive.

You are prompted to reenter the new password.

```
Retype new UNIX password:
```

6. Retype the new password.

The administrator password is updated and a confirmation message appears followed by the Junos Space Settings Menu.

```
passwd: all authentication tokens updated successfully.
```

Changing the Network Settings of a Junos Space Virtual Appliance

NOTE:

- From Junos Space Network Management Platform Release 14.1R2 onward, you can configure Junos Space Ethernet interfaces with only IPv4 addresses, or both IPv4 and IPv6 addresses.
- For a multi-node fabric, we recommend that you modify the network settings by using the Junos Space Network Management Platform GUI.
- From Junos Space Network Management Platform Release 16.1R1 onward, you can configure access to Junos Space through a Network Address Translation (NAT) gateway.

From the Change Network Settings option of the Junos Space Settings Menu, you can perform the following tasks on a Junos Space Virtual Appliance:

- [Adding a DNS Server | 93](#)
- [Deleting a DNS Server | 95](#)
- [Modifying the Virtual IP Address | 96](#)

- [Modifying the IP Address of the eth0 Interface | 100](#)
- [Modifying the NAT Configuration | 106](#)
- [Modifying the IP Address of the eth1 Interface | 111](#)
- [Modifying the IP Address of the eth3 Interface | 113](#)
- [Adding Static Routes to a Junos Space Virtual Appliance | 119](#)
- [Deleting Static Routes from a Junos Space Virtual Appliance | 124](#)

Adding a DNS Server

You can add up to three DNS servers for a Junos Space installation. After each addition, you are redirected to the Junos Space Settings Menu.

To add a DNS server:

1. At the Junos Space Settings Menu prompt, type **2**.

The Change Network Settings menu appears.

```
Change Network Settings:
1> Set DNS Servers
2> Change IP Address of Space node
3> Change Static Routes

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-3,AMR]:
```

NOTE: The **Change IP Address of Space node** option is not provided on the Change Network Settings menu for a standalone node.

2. Type **1** at the prompt.

The DNS name server options menu appears, as shown in the following sample:

```
DNS name server options:

1> Add an IPv4 nameserver
```

```

2> Add an IPv6 nameserver
3> Delete 192.0.2.10
4> Delete 2001:db8:0:1:192:0:2:10

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-3,AMR]:

```

3. Type **1** to add the DNS server by entering the IP address in IPv4 format or type **2** to add the DNS server by entering the IP address in IPv6 format.

4. Type the IP address of the DNS server and press Enter.

Junos Space pings the DNS server. If it is unable to reach the server, it displays a message **Cannot ping ip address**:

```

Cannot ping 192.0.2.11
Use this address? [y/n]

```

5. Type **y** to continue adding the DNS server or **n** to return to the Junos Space Settings Menu.

If you type **y**, the change is queued and the Junos Space Settings Menu appears.

Deleting a DNS Server

You can delete a DNS server if you no longer need it. Use the Set DNS Servers option of the Change Network Settings menu to delete the DNS server.

To delete a DNS server:

1. At the Junos Space Settings Menu prompt, type **2**.

The Change Network Settings menu appears.

```
Change Network Settings:
1> Set DNS Servers
2> Change IP Address of Space node
3> Change Static Routes

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-3,AMR]:
```

2. Type **1** at the prompt.

The DNS name server options menu appears, as shown in the following example:

```
1> Add an IPv4 nameserver
2> Add an IPv6 nameserver
3> Delete 192.0.2.10
4> Delete 2001:db8:0:1:192:0:2:10

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-2,AMR]:
```

3. Type the number present against the DNS server that you want to delete at the prompt; for example, **2**.

You are prompted to confirm that you want to delete the DNS server, as shown in the following sample:

```
Delete nameserver 192.0.2.11? [y/N]
```

4. Type **y** to delete the DNS server or **N** to cancel the operation and return to the Junos Space Settings Menu.

If you type **y**, the DNS server is removed and the Junos Space Settings Menu appears:

```
Removing nameserver 192.0.2.10
```

Modifying the Virtual IP Address

You may need to modify the virtual IP (VIP) address of a Junos Space Virtual Appliance when you move it from one network to another. The virtual appliance reboots after the virtual IP address is modified. For nodes in a Junos Space fabric, you can modify a VIP address from any node in the fabric.

NOTE: The VIP address should be in the same subnet as the eth0 interface.

To modify the virtual IP (VIP) address of a Junos Space Virtual Appliance:

1. At the Junos Space Settings Menu prompt, type **2**.

The Change Network Settings menu appears:

```
Change Network Settings:
1> Set DNS Servers
2> Change IP Address of Space node
3> Change Static Routes

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-3,AMR]: 2
```

2. Type **2** at the prompt.

The Change IP Address of Space Node menu appears.


```

Change IP Address of Space Node:
1> Change VIP
2> Change Node Management Interface
3> Change Device Management Interface
4> Configure NAT

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-4,AMR]: 1

```

3. Type **1** to change the VIP address.

The Change VIP menu appears:

```

Change VIP:
1> Configure IPv4
2> Configure IPv6

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-2,AMR]:

```

NOTE: The Change Device Management Interface option is available only if a device management interface (eth3) was specified during the initial configuration of the appliance.

4. Modify the IP address:

- To modify the IPv4 address:

a. Type **1**.

A confirmation message appears.

```

Change the current VIP(ipv4):192.0.2.53? [y/N]

```

b. Type **y** to continue or **n** to return to the Junos Space Settings Menu.

If you type **y**, you are prompted to enter the new VIP address in dotted-decimal notation.

```
Please type VIP (IPv4) in dotted decimal notation:
```

- c. Type the new VIP address in dotted-decimal notation and press Enter.

The VIP configuration change is queued and the Change IP Address of Space Node menu appears.

- To modify the IPv6 address:

a. Type 2.

The Configuring IPv6 menu and the current IPv6 address configured for VIP are displayed.

```
Configuring IPv6 VIP:
Current VIP(ipv6): 2001:db8:0:1:192:0:3:50

1> Configure
2> Disable

A> Apply changes
M> Return to Main Menu
R> Redraw Menu
```

- i. Type 1 to enter the IPv6 address.
- ii. Type the new IPv6 address for the VIP and press Enter.

```
Please type new VIP(ipv6):
2001:db8:0:1:192:0:3:51
```

The following message appears.

```
VIP configuration change queued. When finished quit (A) to apply changes,
then the system will reboot automatically.
```

- i. Type 2 to disable the IPv6 address of the VIP.

A confirmation message appears:

```
All previously queued changes will be removed immediately. A change to
disable IPv6 VIP will be queued

Do you want to proceed? [y/N]
```



WARNING: If you disable the IPv6 address, the changes queued so far for the IPv6 configuration of VIP are discarded.

- ii. Type y to proceed or N to return to the Change IP Address of the Space Node menu.

If you type **y**, the following message is displayed followed by the Change IP Address of Space Node menu:

```
VIP configuration change queued. When finished quit (A) to apply changes,
then the system will reboot automatically.
```

5. Type **A** to apply the changes or type **M** to return to the Junos Space Settings Menu.

If you type **A**, the Junos Space Virtual Appliance reboots for the VIP address change to take effect.

NOTE: The reboot process can take about 20 minutes to complete.

Modifying the IP Address of the eth0 Interface

You may need to modify the IP address of the node management interface (eth0) of a Junos Space Virtual Appliance when you move it from one network to another. The virtual appliance reboots after the eth0 interface IP address is modified.

To modify the node management interface (eth0) settings of a Junos Space Virtual Appliance:

1. At the Junos Space Settings Menu prompt, type **2**.

The Change Network Settings menu appears:

```
Change Network Settings:
1> Set DNS Servers
2> Change IP Address of Space node
3> Change Static Routes

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-3,AMR]: 2
```

2. Type **2** to change the IP address of the Junos Space Virtual Appliance.

The Change IP Address of Space Node menu appears.

```
Change IP Address of Space Node:
1> Change VIP
```

```
2> Change Node Management Interface
3> Change Device Management Interface
4> Configure NAT

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-4,AMR]: 2
```

3. Type 2 to change the eth0 settings.

The Change Node Management Interface menu appears:

```
Change Node Management Interface:
1> Configure IPv4
2> Configure IPv6

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-2,AMR]: 2
```

4. Modify the IP address of the node management interface:

- To modify the IPv4 address:

a. Type **1**.

The current IPv4 address, network mask, and gateway configured for the eth0 interface and the option to configure the IPv4 address are displayed.

```
Current Node Management Interface IPv4:
```

```
    IP: 192.0.2.50
```

```
Netmask: 255.255.0.0
```

```
Gateway: 192.0.2.150
```

```
1> Configure
```

```
A> Apply changes
```

```
M> Return to Main Menu
```

```
R> Redraw Menu
```

```
Choice [1,AMR]: 1
```

b. Type **1** to modify the IPv4 address of the eth0 interface.

c. Type the new IPv4 address for the eth0 interface in dotted-decimal notation and press Enter.

```
Current IP: 192.0.2.50, please enter new IPv4 address:
```

```
192.0.2.100
```

d. Type the netmask for the eth0 interface in dotted-decimal notation and press Enter.

```
Current Netmask: 255.255.0.0, please enter new Netmask:
```

```
255.255.0.0
```

e. Type the IP address of the gateway in dotted-decimal notation and press Enter.

```
Current Gateway: 192.0.2.150, please enter new IPv4 Gateway:
```

```
192.0.2.150
```

You are prompted to enter the admin password.

f. Type the admin password and press Enter.

The change for the IPv4 address of the eth0 interface is queued and the following confirmation message appears:

Node Management Interface IPv4 configuration change queued.
When finished quit (A) to apply changes, then the system will reboot automatically.

- To modify the IPv6 address:

a. Type 2.

The current IPv6 address, prefix, and gateway configured for the eth0 interface and the options to configure or disable the IPv6 address are displayed.

```
Current Node Management Interface IPv6 :
      IP: 2001:db8:0:1:192:0:2:50
      Prefix: 64
      Gateway: 2001:db8:0:1:192:0:2:150

1> Configure
2> Disable

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-2,AMR]:
```

- i. Type **1** to configure the IPv6 address of the eth0 interface.
- ii. Type the new IPv6 address and prefix for the eth0 interface and press Enter.

```
Current IPv6: 2001:db8:0:1:192:0:2:50/64, please enter new IPv6 address
with new Prefix (IPv6 address/prefix):
2001:db8:0:1:10:192:0:2:100/64
```

- iii. Type the IPv6 address of the gateway for the eth0 interface and press Enter.

```
Current IP: 2001:db8:0:1:192:0:2:150, please enter new IPv6 address:
2001:db8:0:1:192:0:2:150
```

The change to the IPv6 address of the eth0 interface is queued and the following confirmation message appears:

```
Node Management Interface IPv6 configuration change queued.
When finished quit (A) to apply changes, then the system will reboot
automatically
```

- i. Type **2** to disable the IPv6 address on the eth0 interface.

A confirmation message appears:

```
All previously queued changes will be removed immediately. A change to
disable IPv6 on Node Management interface will be queued

Do you want to proceed? [y/N]
```



WARNING: If you disable the IPv6 address, the changes queued so far for the IPv6 address configuration of the eth0 interface are discarded.

- ii. Type **y** to proceed or **N** to return to the Change Node Management Interface menu.

If you type **y**, the following message is displayed followed by the Change IP Address of Space Node menu:

```
IPv6 address disabling on Node Management Interface is queued
When finished quit (A) to apply changes, then the system will reboot
automatically.
```

5. Type **A** to apply the changes or type **M** to return to the Junos Space Settings Menu.

If you type **A**, the Select a change to cancel it menu appears, as shown in the following sample:

```
Select a change to cancel it:
1> NodeIP:192.0.2.100, NodeMask: 255.255.0.0, NodeGateway: 192.0.2.150
2> NodeIP(v6): 2001:db8:0:1:192:0:2:100, NodePrefix(v6): 64, NodeGateway(v6):
2001:db8:0:1:192:0:2:150

A> Apply all changes
M> Make more changes
C> Cancel all changes and quit
R> Redraw Menu

Choice [1-3,AMCR]: A
```

6. Type **A** to apply all the changes or type **C** to cancel modifying the IP address of the eth0 interface, or type a number from the menu to cancel the change. For example, type **2** to discard the IPv6 changes for the eth0 interface.

If you type **A**, the Junos Space Virtual Appliance reboots for the new eth0 interface settings to take effect.

NOTE: The reboot process can take about 20 minutes to complete.

Modifying the NAT Configuration

You may need to modify the NAT configuration of a Junos Space Virtual Appliance when you move it from one network to another.

To modify the NAT configuration of a Junos Space Virtual Appliance:

1. At the Junos Space Settings Menu prompt, type **2**.

The Change Network Settings menu appears:

```
Change Network Settings:
1> Set DNS Servers
2> Change IP Address of Space node
3> Change Static Routes

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-3,AMR]: 2
```

2. Type **2** to change the IP address of the Junos Space Virtual Appliance.

The Change IP Address of Space Node menu appears.

```
Change IP Address of Space Node:
1> Change VIP
2> Change Node Management Interface
3> Change Device Management Interface
4> Configure NAT

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-4,AMR]:
```

NOTE: The NAT configuration option is displayed even if NAT settings are not specified during the initial configuration of the node. If the node is configured to be part of a Junos Space cluster, but is not yet added to the cluster from the Junos Space Platform UI, you can modify only the NAT configuration.

In that case, the following menu appears:

```
Change IP Address of Space Node:
1> Configure NAT

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1,AMR]:
```

3. Depending on the menu options displayed, type **4** or **1**, to modify the NAT configuration.

NOTE: The NAT configuration must not be modified in combination with the other changes that require a reboot of the node. If the node is rebooted, the NAT configuration is discarded. In such cases, modify the settings that require a reboot, reboot the node and then modify the NAT configuration.

The Configuring NAT menu appears:

```
Configuring NAT:

1> Configure IPv4
2> Configure IPv6
3> Configure Both IPv4 and IPv6

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-3,AMR]:
```

4.

NOTE: If you modify only the NAT IPv4 or IPv6 address of a virtual appliance configured to be part of a Junos Space cluster, but yet to be added to the cluster from the Junos Space Platform UI, the last specified IP address overwrites the IP address configured during initial configuration. For example, if the virtual appliance was initially configured with a NAT IPv4 address and while modifying the network settings, you specify an IPv6 address, then the IPv4 address is discarded and the IPv6 address is used for the NAT gateway. If both IPv4 and IPv6 are configured initially, then only the IP address that is modified is updated.

- To configure the IPv4 address:

a. Type **1** and press Enter.

b. Type the IPv4 address of the NAT outbound SSH interface and press Enter.

The IP address must be in the range 1.0.0.1 - 223.255.255.254 excluding 127.x.x.x.

```
Configuring NAT :
```

```
Configuring IPV4 Outbound SSH for NAT:
```

```
Please enter the NAT Outbound SSH IP Address
192.168.190.7
```

c. Type the port number of the NAT outbound SSH interface and press Enter.

The port number must be in the range 0-65535.

```
Please enter the NAT Outbound SSH Port Number
4545
```

d. Type the IPv4 address of the NAT trap interface and press Enter.

The IP address must be in the range 1.0.0.1 - 223.255.255.254 excluding 127.x.x.x.

```
Configuring IPV4 Trap for NAT:
```

```
Please enter the NAT Trap IP Address
192.168.27.1
```

e. Type the port number of the NAT trap interface and press Enter.

The port number must be in the range 0-65535.

```
Please enter the NAT Trap Port Number
4584
```

- To configure the IPv6 address:
 - a. Type **2** and press Enter.
 - b. Type the IPv6 address of the NAT outbound SSH interface and press Enter.

```
Configuring NAT :

Configuring IPV6 OutboundSSH for NAT:

Please enter the NAT Outbound SSH IP Address
2001:db8:85a3::8a2e:130:0:2
```

- c. Type the port number of the NAT outbound SSH interface and press Enter.
The port number must be in the range 0-65535.

```
Please enter the NAT Outbound SSH Port Number
5054
```

- d. Type the IPv6 address of the NAT trap interface and press Enter.

```
Configuring IPV6 Trap for NAT:

Please enter the NAT Trap IP Address
2001:db8:85a3::8a2e:130:0:2
```

- e. Type the port number of the NAT trap interface and press Enter.
The port number must be in the range 0-65535.

```
Please enter the NAT Trap Port Number

5054
```

- To configure IPv4 and IPv6:

a. Type **3** and press Enter.

b. Type the IPv4 address of the NAT outbound SSH interface and press Enter.

The IP address must be in the range 1.0.0.1 - 223.255.255.254 excluding 127.x.x.x.

```
Configuring IPV4 OutboundSSH for NAT:
```

```
Please enter the NAT Outbound SSH IP Address
```

```
192.168.190.7
```

c. Type the port number of the NAT outbound SSH interface and press Enter.

The port number must be in the range 0-65535.

```
Please enter the NAT Outbound SSH Port Number
```

```
4545
```

d. Type the IPv4 address of the NAT trap interface and press Enter.

The IP address must be in the range 1.0.0.1 - 223.255.255.254 excluding 127.x.x.x.

```
Configuring IPV4 Trap for NAT:
```

```
Please enter the NAT Trap IP Address
```

```
192.168.27.1
```

e. Type the port number of the NAT trap interface and press Enter.

The port number must be in the range 0-65535.

```
Please enter the NAT Trap Port Number
```

```
4584
```

f. Type the IPv6 address of the NAT outbound SSH interface and press Enter.

```
Configuring IPV6 OutboundSSH for NAT:
```

```
Please enter the NAT Outbound SSH IP Address
```

```
2001:db8:85a3::8a2e:130:0:2
```

g. Type the port number of the NAT outbound SSH interface and press Enter.

The port number must be in the range 0-65535.

```
Please enter the NAT Outbound SSH Port Number
7075
```

- h. Type the IPv6 address of the NAT trap interface and press Enter.

```
Configuring IPV6 Trap for NAT:

Please enter the NAT Trap IP Address
2001:db8:85a3::8a2e:130:0:2
```

- i. Type the port number of the NAT trap interface and press Enter.

The port number must be in the range 0-65535.

```
Please enter the NAT Trap Port Number
7076
```

5. Type **A** and press Enter to apply the changes.

The settings summary is displayed.

6. Type **A** again and press Enter to accept and apply all the changes.

The Junos Space Settings menu appears.

Modifying the IP Address of the eth1 Interface

You may need to modify the IP address of the eth1 interface of a Junos Space or an FMPPM node when you move the Junos Space or FMPPM node from one network to another.

NOTE:

- From Junos Space Network Management Platform Release 14.1R1 onward, you can configure the eth1 Ethernet interface as an administrative interface.
- If you configure the eth1 interface, SSH is disabled on the eth0 and the eth3 interfaces. You can then access the CLI of the Junos Space virtual appliance only through the eth1 interface.

To modify the eth1 interface settings:

1. On the Junos Space Settings Menu, type **7** to access shell.

You are prompted to enter your password.

2. Type your password and press Enter.

The shell prompt appears.

3. At the shell prompt, type **jmp_config** and press Enter.

You are prompted to enter the IP address of the eth1 interface.

4. Type the IP address of the eth1 interface in dotted-decimal notation and press Enter.

The IP address can be in the same subnet as virtual IP (VIP) address or in a different subnet. If the IP address is not in the same subnet as the VIP address, you are prompted to enter the subnet mask and then the default gateway for the eth1 interface.

5. (Optional) Type the subnet mask for the eth1 interface in dotted-decimal notation and press Enter.

6. (Optional) Type the default gateway in dotted-decimal notation and press Enter.

The eth1 interface is configured.

7. To verify the modified IP address of the eth1 interface, run the **ifconfig eth1** command and check that the IP address displayed for eth1 is the same as that you modified.

Modifying the IP Address of the eth3 Interface

You may need to modify the eth3 interface IP address of a Junos Space Virtual Appliance when you move it from one network to another. The virtual appliance reboots after the eth3 interface IP address is modified.

NOTE:

- On a Junos Space fabric with two or more Junos Space nodes, if you configure the eth3 interface as the device management interface on one Junos Space node, then you must also configure the eth3 interface as the device management interface on all the other Junos Space nodes in that fabric.
- When you configure the eth3 interface as the device management interface, the IP addresses of the eth0 and eth3 Ethernet interfaces must be in different subnets.

To modify the device management interface (eth3) settings of a Junos Space Virtual Appliance:

1. At the Junos Space Settings Menu prompt, type **2**.

The Change Network Settings menu appears:

```
Change Network Settings:
1> Set DNS Servers
2> Change IP Address of Space node
3> Change Static Routes

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-3,AMR]: 2
```

2. Type **2** to change the IP address of the Junos Space Virtual Appliance.

The Change IP Address of Space node appears.

```
Change IP Address of Space node:
1> Change VIP
2> Change Node Management Interface
3> Change Device Management Interface
4> Configure NAT

A> Apply changes
M> Return to Main Menu
```

```
R> Redraw Menu

Choice [1-4,AMR]: 3
```

3. Type **3** to change the Device Management Interface (eth3) settings.

The Change Device Management Interface menu appears.

```
Change Device Management Interface:
1> Configure IPv4
2> Configure IPv6

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-2,AMR]: 1
```

4. Modify the IP address of the device management interface:

- To modify the IPv4 address of the eth3 interface
 - a. Type **1**.

The current IPv4 address, network mask, and gateway configured for the eth3 interface and the options to configure or disable the IPv4 address of the eth3 interface are displayed.

```
Current Device Management Interface IPv4 :
    IP: 192.0.2.60
Netmask: 255.255.0.0
Gateway: 192.0.2.158

1> Configure
2> Disable

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1,AMR]:
```

- b. • i. Type **1** to modify the IPv4 address of the eth3 interface.

- ii. Type the IPv4 address for the eth3 interface in dotted-decimal notation and press Enter.

```
Current IP: 192.0.2.60 please enter new IPv4 address:
192.0.2.55
```

- iii. Type the network mask for the eth3 interface in dotted-decimal notation and press Enter.

```
Current Netmask: 255.255.0.0, please enter new Netmask:
255.255.0.0
```

- iv. Type the IP address of the gateway in dotted-decimal notation and press Enter.

```
Current Gateway: 192.0.2.158, please enter new IPv4 Gateway:
192.0.2.160
```

- v. Type the admin password and press Enter.

The change for the IPv4 address of the eth3 interface is queued and the following confirmation message appears:

```
Device Management Interface IPv4 configuration change queued.
When finished quit (A) to apply changes, then the system will reboot
automatically.
```

- i. Type **2** to disable the IPv4 address on the eth3 interface.

A confirmation message appears:

```
All previously queued changes will be removed immediately.
Do you want to proceed? [y/n]
```



WARNING: If you choose to disable the IPv4 address on the eth3 interface, the changes queued so far for the IPv4 address configuration of the eth3 interface are discarded.

- ii. Type **y** to proceed or **n** to return to the Change Device Management Interface menu.

If you type **y**, the following message is displayed followed by the Change Device Management Interface menu:

```
IPv4 address disabling on Device Management Interface is queued  
When finished quit (A) to apply changes, then the system will reboot  
automatically.
```

- To modify the IPv6 address:

a. Type **1**.

The current IPv6 address configured for the eth3 interface is displayed followed by the options to configure and disable the IPv6 address.

```
Current Device Management Interface IPv6:
```

```
    IP: 2001:db8:20:192:0:2:50
```

```
    Prefix: 64
```

```
Gateway: 2001:db8:20:1:192:0:2:150
```

```
1> Configure
```

```
2> Disable
```

```
A> Apply changes
```

```
M> Return to Main Menu
```

```
R> Redraw Menu
```

```
Choice [1-2,AMR]:
```

- i. Type **1** to configure the IPv6 address of the eth3 interface.

You are prompted to enter the IPv6 address for the eth3 interface.

- ii. Type the new IPv6 address and prefix for the eth3 interface and press Enter.

```
Current IP: 2001:db8:20:1:192:0:2:50/64, please enter new IPv6 address
with new Prefix (IPv6 Address/prefix):
2001:db8:20:1:192:0:2:55/64
```

- iii. Type the IPv6 address of the gateway for the eth3 interface and press Enter.

```
Current Gateway: 2001:db8:20:192:0:2:150, please enter new IPv6 Gateway:
2001:db8:20:192:0:2:150
```

The following message appears:

```
Device Management Interface IPv6 configuration change queued.
When finished quit (A) to apply changes, then the system will reboot
automatically
```

- i. Type **2** to disable the IPv6 address on the eth3 interface.

A confirmation message appears:

```
All previously queued changes will be removed immediately.
Do you want to proceed? [y/n]
```



WARNING: If you disable IPv6 address, the changes queued so far the IPv6 address configuration of the eth3 interface are discarded.

- ii. Type **y** to proceed or **n** to return to the Change Device Management Interface menu.

If you type **y**, the following message is displayed followed by the Change Device Management Interface menu.

```
IPv6 address disabling on Device Management Interface is queued.
When finished quit (A) to apply changes, then the system will reboot
automatically.
```

```
Change Device Management Interface:
```

```
1> Configure IPv4
```

```
2> Configure IPv6
```

```
A> Apply changes
```

```
M> Return to Main Menu
```

```
R> Redraw Menu
```

```
Choice [1-2,AMR]:
```

5. Type **A** to apply the changes or type **M** to return to the Junos Space Settings Menu.

If you type **A**, the Select a change to cancel it menu appears, as shown in the following example:

```
Select a change to cancel it:
```

```
1> DEVIP:192.0.2.55, DEVMask:255.255.0.0, DEVGateway:192.0.2.160
2> DEVIP(v6): 2001:db8:20:1:192:0:2:55, DEVPrefix(v6): 64, DEVGateway(v6):
2001:db8:20:1:192:0:2:150
```

```
A> Apply all changes
M> Make more changes
C> Cancel all changes and quit
R> Redraw Menu
```

```
Choice [1,AMCR]:
```

6. Type **A** to apply the changes, or type **C** to cancel modifying the IP address settings of the eth3 interface, or type a number from the menu to cancel the change. For example, type **1** to discard the changes to the IPv4 address, the network mask, and the gateway IP address of the eth3 interface.

If you type **A**, the Junos Space Virtual Appliance reboots for the new eth3 interface settings to take effect.

NOTE: The reboot process can take about 20 minutes to complete.

Adding Static Routes to a Junos Space Virtual Appliance

Before you add a static route to a Junos Space Virtual Appliance, ensure that the gateway that you want to configure is accessible.

To add a static route to a Junos Space Virtual Appliance:

1. At the Junos Space Settings Menu prompt, type **2**.

The Change Network Settings menu appears.

```
Change Network Settings:
1> Set DNS Servers
2> Change IP Address of Space node
3> Change Static Routes

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-3,AMR]:
```

2. Type **3** at the prompt.

The Change Static Routes menu appears.

```
Change Static Routes:
1> IPv4 Routes
2> IPv6 Routes

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-2,AMR]:
```

3. Modify static routes.

- a. To change IPv4 static routes, type **1**.

The option to add a new static route appears.

```
1> Add new static route

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1,AMR]: 1
```

- b. Type **1**.

You are prompted to enter the IPv4 address of the new static route.

- c. Type the IP address of the static route in dotted-decimal notation and press Enter.

```
Adding static route:
Please enter the destination network:
192.0.2.40
```

- d. Type the network mask for the route in dotted-decimal notation and press Enter.

```
Please enter the subnet mask in dotted decimal notation:
255.255.0.0
```

- e. Type the gateway for the route in dotted-decimal notation and press Enter.

```
Please enter the gateway for this route:
192.0.2.151
```

- f. Type the password for the admin user and press Enter.

The change is queued and you get a confirmation message.

```
Static Route configuration change queued. When finished quit (A) to apply
changes

Change queued:
```

```
Add->192.0.2.40/255.255.0.0->eth0:192.0.2.151
```

```
1> Add new static route
```

```
A> Apply changes
```

```
M> Return to Main Menu
```

```
R> Redraw Menu
```

- a. To change IPv6 static routes, type 2.

The option to enter a new IPv6 static route appears.

```
1> Add new static route
```

```
A> Apply changes
```

```
M> Return to Main Menu
```

```
R> Redraw Menu
```

```
Choice [1,AMR]: 1
```

- b. Type 1.

- c. Type the IPv6 address of destination network without prefix and press Enter.

```
Adding IPv6 static route:
```

```
Please enter the destination network (without prefix):
```

```
2001:db8:40:1:0:0:0:0
```

- d. Type the prefix for the route and press Enter.

```
Please enter the prefix:
```

```
64
```

- e. Type the gateway for the route in dotted-decimal notation and press Enter.

```
Please enter the gateway for this route:
```

```
2001:db8:40:1:192:0:2:151
```

Junos Space pings the IP address that you entered. If Junos Space is unable to reach the gateway, it reports the following:

```
Cannot ping 2001:db8:0:1:192:0:2:151
Use this address? [y/N]
```

Type **y** to continue or **n** to return to Junos Space settings menu.

If you enter **y**, you are prompted to enter password for the admin user.

- f. Type the password for the admin user and press Enter.

The change is queued and you get a confirmation message.

```
Static Route configuration change queued. When finished quit (A) to apply
changes

Change  queued:
Add->2001:db8:40:1:0:0:0:0/64->eth0-2001:db8:0:1:192:0:2:151
1> Add new static route

A> Apply changes
M> Return to Main Menu
R> Redraw Menu
```

4. Type **A** to apply changes are **M** to return to the Junos Space Settings menu.

Deleting Static Routes from a Junos Space Virtual Appliance

You can delete static routes from the Junos Space Virtual Appliance when you no longer need them.

To delete a static route from a Junos Space Virtual Appliance:

1. At the Junos Space Settings Menu prompt, type **2**.

The Change Network Settings menu appears.

```
Change Network Settings:
1> Set DNS Servers
2> Change IP Address of Space node
3> Change Static Routes

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-3,AMR]:
```

2. Type **3** at the prompt.

The Change Static Routes menu appears.

```
Change Static Routes:
1> IPv4 Routes
2> IPv6 Routes

A> Apply changes
M> Return to Main Menu
R> Redraw Menu
```

The options to modify static routes appear, as shown in the following example:

3. • Delete the static routes.

- a. To delete IPv4 routes, type **1**.

A menu appears with options to add and remove IPv4 static routes similar to the following sample:

```

1> Add new static route
2> Remove->192.0.2.40/255.255.0.0->eth0:192.0.2.151

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-4,AMR]:

```

- b. At the prompt, type the number provided against the static route you want to delete. For example, **2**.

You are prompted to apply or cancel deleting the static route, as shown in the following sample:

```

1> Remove-->192.0.2.40/255.255.0.0->eth0:192.0.2.151

A> Apply all changes
M> Make more changes
C> Cancel all changes and quit
R> Redraw Menu

Choice [1,AMCR]: A

```

- Delete the IPv6 routes.

- a. To delete IPv6 routes, type **2**.

A menu appears with options to add and remove IPv6 static routes similar to the following:

```

1> Add new static route
2> Remove->2001:db8:40:1:0:0:0:0/64->eth0-2001:db8:0:1:192:0:2:151

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-4,AMR]:

```

- b. At the prompt, type the number provided against the static route you want to delete. For example, **2**.

You are prompted to apply or cancel deleting the static route, as shown in the following example:

```

1> Remove->2001:db8:40:1:0:0:0:0/64->eth0-2001:db8:0:1:192:0:2:151

A> Apply all changes
M> Make more changes
C> Cancel all changes and quit
R> Redraw Menu

Choice [1,AMCR]: A

```

4. Type **A** to delete the static route or **M** to make more changes.

If you type **A**, you are prompted to enter the administrator password and then the static route is deleted.

Changing Time Options of a Junos Space Virtual Appliance

Change Time Options enables you to change the time zone and NTP server settings of a Junos Space Virtual Appliance. When you configure each Junos Space Virtual Appliance with an NTP server, you must ensure that, if the first node (which is used to synchronize time for all nodes in the fabric) goes down, all other nodes in the fabric remain synchronized. To ensure this behavior, all nodes in the fabric should be configured with the same external NTP source that you configured for the first appliance.

- [Changing the Time Zone | 126](#)
- [Changing NTP Settings | 128](#)

Changing the Time Zone

Use the Change Timezone option of the Change Time Options menu to change the time zone of the Junos Space Virtual Appliance.

To change the time zone of a Junos Space Virtual Appliance:

1. At the Junos Space Settings Menu prompt, type **3**.

The Change Time Options menu appears:

```

Change Time Options:
1> Change Timezone
2> Change NTP options

A> Apply changes

```

```
M> Return to Main Menu
R> Redraw Menu
```

2. Type **1** at the prompt.

The current time zone configured on the Junos Space Virtual Appliance is displayed and you are prompted to choose the time zone that you want to set, as shown in the following example:

```
Current Time Zone is: "Etc/UTC"
```

```
1> GMT
2> Africa
3> America
4> Antarctica
5> Arctic
6> Asia
7> Atlantic
8> Australia
9> Europe
10> Indian
11> Pacific

A> Apply changes
M> Return to Main Menu
R> Redraw Menu
```

```
Choice [1-11,AMR]:
```

3. Type the number against the time zone that you want to set; for example, type **1** for GMT. If the time zone has associated locations, you are prompted to enter the location. For example, the Atlantic time zone has the following locations:

```
1> Antananarivo
2> Chagos
3> Christmas
4> Cocos
5> Comoro
6> Kerguelen
7> Mahe
8> Maldives
```

```

9> Mauritius
10> Mayotte
11> Reunion

```

4. Type the number against the location that you want to set.

You are prompted to confirm the time zone that you want to set.

```

Set TimeZone to Indian/Maldives? [y/N]

```

5. Type **y** to confirm or **N** to return to the Junos Space Settings Menu.

Changing NTP Settings

Changing Network Time Protocol (NTP) settings involves disabling or enabling NTP on a Junos Space Virtual Appliance, adding NTP servers to a Junos Space Virtual Appliance, or deleting NTP servers configured on the Junos Space Virtual Appliance.

To change NTP settings of a Junos Space Virtual Appliance:

1. At the Junos Space Settings Menu prompt, type **3**.

The Change Time Options menu appears:

```

Change Time Options:
1> Change Timezone
2> Change NTP options

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

```

2. Type **2** to change NTP options.

The NTP options menu appears.

```

NTP options:
1> Disable NTP
2> Add an NTP server

A> Apply changes
M> Return to Main Menu

```



```
R> Redraw Menu

Choice [1-2,AMR]:
```

If there are NTP servers already configured on the Junos Space Virtual Appliance, they are listed on the NTP options menu.

```
NTP options:
1> Disable NTP
2> Add an NTP server
3> Delete device1.example.com

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-3,AMR]:
```

3. Perform one of the following tasks:

- Type **1** to disable NTP on the Junos Space Virtual Appliance.

The Junos Space Settings Menu appears.

NTP is enabled by default on the Junos Space Virtual Appliance. If NTP is disabled, typing **1** enables it.

- Type **2** to add an NTP server to the Junos Space Virtual Appliance.

You are prompted to enter the IP address or hostname of the NTP server.

- a. Type the IP address or hostname of the NTP server at the prompt.

A message confirming the addition of the NTP server appears followed by the Junos Space Settings Menu.

- b. Type **A** to apply the settings.

- Type the number against a configured NTP server to delete it from the Junos Space Virtual Appliance.

You are prompted to confirm that you want to delete the NTP server.

```
3> Delete NTP server device1.example.com? [y/N]
```

Type **y** to delete or **N** to return to the Junos Space Settings Menu.

Retrieving System Log Files from a Junos Space Virtual Appliance

To retrieve system log files from a Junos Space Virtual Appliance, you can use Secure Copy Protocol (SCP) if the network is functional or a USB device if the network is down.

NOTE: To save the system log files of a device in a USB device, the device must be connected to the Junos Space Virtual Appliance.

To retrieve system log files from a Junos Space Virtual Appliance:

1. At the Junos Space Settings Menu prompt, type **4**.

The following appears:

```
1> Save to USB Device
2> Send Using SCP

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-2,AMR]:
```

2. Choose a method for retrieving system log files—using a USB device or SCP:

- Retrieving log files using a USB device

To save system log files to a USB device:

- a. Type **1** at the prompt.

You are prompted to confirm that you want to copy the files onto a USB device.

```
This process will retrieve the log files on all cluster members
and combine them into a .tar file. Once the file is created, you
can copy the files onto a USB drive.
Continue? [y/n]
```

- b. Type **y** to continue with retrieving the logs or **n** to return to the Junos Space Settings Menu.

If you type **y**, you are prompted for the administrator password.

```
Local admin password:
```

- c. Type the administrator password of this Junos Space installation and press Enter.

You are prompted to confirm that the logs can be saved on the USB device.

```
Log collection complete
If USB key is ready, press "Y". To abort, press "N".
```

- d. Type **Y** to save the log files to your USB device or **N** to terminate collecting logs and return to the Junos Space Settings Menu.

The Junos Space Network Management Platform retrieves the log files from all cluster members as a single tar file.

- Retrieving system log files using SCP

To save system log files using SCP:

- a. Type **2** at the prompt.

You are prompted to confirm that you want to use SCP to save the system log files.

```
This process will retrieve the log files on all cluster members
and combine them into a .tar file. Once the file is created, you
will be asked for a remote scp server to transfer the file to.
Continue? [y/n]
```

- b. Type **y** to continue with retrieving the system log files or **n** to terminate and return to the Junos Space Settings Menu.

You are prompted to enter the administrator password.

```
Local admin password:
```

- c. Type the administrator password of this Junos Space installation and press Enter.

You are prompted for the credentials of the SCP server where you want to save the system log files, starting with the IP address.

```
Please enter remote scp server IP address:
```

- d. Type the SCP server IP address and press Enter.

You are prompted to enter the username to log in to the SCP server.

```
Please enter remote scp user:
```

- e. Type the SCP server username and press Enter.

You are prompted to enter the location in the SCP server where you want to store the system log files.

```
Please enter remote scp file location:
```

- f. Type the path in the SCP server where you want to save the system log files and press Enter.

You are prompted to confirm the credentials of the SCP server that you have entered so far, as shown in the following example:

```
Remote scp IP: 192.168.1.2
Remote scp user: admin
Remote scp path: C:Users/admin/desktopi
Is this correct? [y/n]
```

- g. Type **y** to confirm or **n** to reenter the credentials of the SCP server.

If you type **y**, the log files are saved in the specified location of the SCP server as a single tar file.

Expanding the Drive Size of a Junos Space Virtual Appliance

To increase the virtual machine (VM) drive size on a Junos Space Virtual Appliance, you must first add a disk resource to the VMware Infrastructure client to create a virtual disk. You must then initiate a scan of the new virtual disk. The Expand VM Drive Size option does not expand the drive size. If you increase the size of any disk on the Virtual Appliance (for example, using the Edit menu of the vSphere Client). To expand the drive size, you must add disk resources to the host system.

The free space available in all the partitions should be monitored periodically and the available disk space should be increased if required. The **/var** and **/var/log** partitions should be monitored more frequently as most of the data are stored in these partitions and the space utilization is high.

NOTE: You can expand the VM drive size of a Junos Space Virtual Appliance only when the Junos Space Virtual Appliance is powered on.

To expand the VM drive size of a Junos Space Virtual Appliance:

1. At the Junos Space Settings Menu prompt, type **6**.

You are prompted to enter the password for the admin user.

NOTE: If no free space is available on the host for allocation, the **No free disk space** message appears and the Junos Space Settings Menu is displayed.

2. Type the password for the admin user and press Enter.

The following caution appears and you are prompted to confirm that you want to continue expanding the VM drive size.

```
-----Caution-----
Expanding Disk drives would restart Jboss and MySQL processes, all the GUI users
would be logged out automatically.
Note: This will cause Space Fabric to failover to other node.
Do you want to continue? [y/n]
```

3. Type **y** to continue with the procedure or **n** to return to the Junos Space Settings Menu.

If you type **y**, you are prompted to specify the partition that you want to expand.

```
Begin to stop Jboss and MySQL...
Service Jboss and MySQL stopped

Which partition do you want to expand?
1) /
2) /var
3) /var/log
4) /tmp
5) Quit
Select a partition: 1
```

4. Type the number present against the partition that you want to expand; for example, type **1** to expand the / partition or **5** to quit expanding disks and return to the Junos Space Settings Menu.

The free space that can be allocated is displayed and you are prompted to enter the space that you want to allocate to the partition.

```
Current disk partition size of / is 22G
Total 4.97G free disk space can be allocated

How much additional disk space is to be added(Acceptable suffixes: M|G|T): 1M
```

5. Type the additional disk space that you want to allocate and press Enter.

You can enter the disk space in megabytes (M), gigabytes (G), or terabytes (T). Do not add a space between the number and the unit; for example, 50M and not 50 M, 10G and not 10 G, and so on.

You are prompted whether you want to expand more drives.

```
Increasing size of LV /dev/jmpvgnocf/lvroot
  Extending logical volume lvroot to 22.59 GB
  Logical volume lvroot successfully resized
Resizing / onto new space, this will take a few minutes
resize4fs 1.41.12 (17-May-2010)
Filesystem at /dev/jmpvgnocf/lvroot is mounted on /; on-line resizing required
old desc_blocks = 2, new_desc_blocks = 2
Performing an on-line resize of /dev/jmpvgnocf/lvroot to 5922816 (4k) blocks.
The filesystem on /dev/jmpvgnocf/lvroot is now 5922816 blocks long.

4.94G free disk space available
Do you want to expand more disks? [y/N]
```

6. Type **y** to continue adding disk space or **n** to return to the Junos Space Settings Menu.

When you type **n**, the JBoss and MySQL processes that were stopped are resumed. If the VM drive size was expanded on a primary node, the node becomes secondary when it comes up.

Setting Security Options on a Junos Space Virtual Appliance

Junos Space provides firewall and SSH security options. By default, the firewall and SSH are enabled on a Junos Space Virtual Appliance.

- [Enabling the Firewall on a Junos Space Virtual Appliance | 135](#)
- [Disabling the Firewall on a Junos Space Virtual Appliance | 136](#)
- [Disabling SSH on a Junos Space Virtual Appliance | 136](#)
- [Enabling SSH on a Junos Space Virtual Appliance | 137](#)

Enabling the Firewall on a Junos Space Virtual Appliance

You can disable the firewall if you want and then reenabling it.

To enable the firewall on a Junos Space Virtual Appliance:

1. At the Junos Space Settings Menu prompt, type 5.

The following appears if the firewall is disabled and SSH is enabled:

```
1> Enable Firewall
2> Disable SSH

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-2,AMR]:
```

2. Type 1.

You are prompted to enter the administrator password.

```
Password:
```

3. Type the administrator password and press Enter.

The following appears and the firewall is enabled on the Junos Space Virtual Appliance:

```
Starting jmp-firewall: [ OK ]
```

Disabling the Firewall on a Junos Space Virtual Appliance

By default, the firewall is enabled on a Junos Space Virtual Appliance. You can disable the firewall if you want.

To disable the firewall on a Junos Space Virtual Appliance:

1. At the Junos Space Settings Menu prompt, type **5**.

The following appears if both the firewall and SSH are enabled:

```
1> Disable Firewall
2> Disable SSH

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-2,AMR]:
```

2. Type **1**.

You are prompted to enter the administrator password.

```
Password:
```

3. Type the administrator password and press Enter.

The following appears and the firewall is disabled on the Junos Space Virtual Appliance:

```
Stopping jmp-firewall:
Flushing firewall rules:           [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules:       [ OK ]
```

Disabling SSH on a Junos Space Virtual Appliance

By default, SSH is enabled on a Junos Space Virtual Appliance. You can disable SSH if you want.

To disable SSH on a Junos Space Virtual Appliance:

1. At the Junos Space Settings Menu prompt, type **5**.

The following appears if both the firewall and SSH are enabled:


```

1> Disable Firewall
2> Disable SSH

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-2,AMR]:

```

2. Type 2.

You are prompted for the administrator password.

```

Password:

```

3. Type the administrator password and press Enter.

The following appears and SSH is disabled on the Junos Space Virtual Appliance.

```

Stopping sshd:                                     [ OK ]

```

Enabling SSH on a Junos Space Virtual Appliance

By default, SSH is enabled on a Junos Space Virtual Appliance. You can disable SSH if you want and then enable it again.

To enable SSH on a Junos Space Virtual Appliance:

1. At the Junos Space Settings Menu prompt, type 5.

The following appears when the firewall is enabled and SSH is disabled::

```

1> Disable Firewall
2> Enable SSH

A> Apply changes
M> Return to Main Menu
R> Redraw Menu

Choice [1-2,AMR]:

```

2. Type 2.

You are prompted for the administrator password.

```
Password:
```

3. Type the administrator password and press Enter.

The following appears and SSH is enabled on the Junos Space Virtual Appliance.

```
Starting sshd: [ OK ]
```

Running Shell in a Junos Space Virtual Appliance

You must initialize shell to access the CLI and run commands to debug a Junos Space Virtual Appliance.

To run shell in the Junos Space Virtual Appliance:

1. At the Junos Space Settings Menu prompt, type 7.

You are prompted for the administrator password.

2. Type the current administrator password and press Enter.

The CLI prompt of the Junos Space Virtual Appliance appears, as shown in the following example:

```
[root@host ~]#
```

RELATED DOCUMENTATION

[Downloading Troubleshooting System Log Files Through the Junos Space CLI](#)

[Ethernet Interfaces in a Junos Space Virtual Appliance Overview](#) | 13

4

CHAPTER

Viewing and Adding Nodes to a Fabric

Adding a Node to an Existing Junos Space Fabric | **141**

Viewing Nodes in the Fabric | **150**

Adding a Node to an Existing Junos Space Fabric

IN THIS SECTION

- [Adding a Junos Space Node to the Junos Space Fabric | 142](#)
- [Adding an FMPM Node to the Junos Space Fabric | 147](#)
- [Obtaining Fingerprint of a Junos Space Node | 149](#)

When you configure a JA2500 Junos Space Appliance (JA2500) or a Junos Space Virtual Appliance as a Junos Space node by using the Junos Space CLI, Junos Space Network Management Platform automatically adds the first node to the fabric. By default, the Junos Space fabric contains this single node that provides complete Junos Space Platform functionality. For each additional node that you install and configure, you must add the node from the Junos Space Platform UI to represent the node in the fabric.

Before you begin, the following prerequisites must be in place:

- Multicast must be enabled on the switches to which Junos Space nodes are connected.
- IGMP-snooping needs to be disabled on the switches to which Junos Space nodes are connected. By default, IGMP-snooping is enabled on most switches.
- All Junos Space nodes must be interconnected using a high-speed (1-Gbps or 100-Mbps) network with a maximum latency not exceeding 300 milliseconds.

Using the Junos Space CLI, you can configure a Junos Space Appliance or a Junos Space Virtual Appliance either as a Junos Space node or a Fault Monitoring and Performance Monitoring (FMPM) node. If you want to add a node to the fabric as a dedicated database node or a dedicated Cassandra node, it must be configured as a Junos Space node.

For information about how to configure a Junos Space Virtual Appliance as a Junos Space node, see [“Configuring a Junos Space Virtual Appliance as a Junos Space Node” on page 43](#) in the *Junos Space Virtual Appliance Installation and Configuration Guide* and for information about how to configure a JA2500 appliance as a Junos Space node, see *Configuring a Junos Space Appliance as a Junos Space Node* in the *JA2500 Junos Space Appliance Hardware Guide*.

For information about how to configure a Junos Space Virtual Appliance as an FMPM node, see [“Configuring a Junos Space Virtual Appliance as a Standalone or Primary FMPM Node” on page 70](#) or [“Configuring a Junos Space Virtual Appliance as a Backup or Secondary FMPM Node for High Availability” on page 81](#) in the *Junos Space Virtual Appliance Installation and Configuration Guide*. For information about how to configure a JA2500 appliance as an FMPM node, see *Configuring a Junos Space Appliance as a Standalone*

or Primary FMPM Node or Configuring a Junos Space Appliance as a Backup or Secondary FMPM Node for High Availability in the JA2500 Junos Space Appliance Hardware Guide.

NOTE: If you want to change an existing Junos Space node to an FMPM node or vice versa, you must reimage the appliance and reconfigure it as an FMPM node or a Junos Space node. For more information, refer to the Junos Space Appliance and Junos Space Virtual Appliance documentation.

NOTE:

Before you add a node to the Junos Space fabric, verify the following:

- The version of Junos Space Platform installed on the node is the same as the version installed on other nodes in the fabric.
- Ensure that no jobs are pending.
- If a Junos Space node, a database node, or an FMPM node that is part of an existing fabric is deleted, then you need to reimage the node before the node can be readded to the fabric. Junos Space displays the following message when you try to add such nodes to an existing fabric:
The node you are trying to add was part of another fabric, please re-image the node before adding to this fabric.
- Ensure that you are not adding a non-FMPM node as an FMPM node. Junos Space Platform displays the following message when you try to add such a node to the fabric:
Node agent is not running on {0}. Please make sure the node being added is not a specialized node.

From the Junos Space Platform UI, you can add a node to the Junos Space fabric by executing one of the following procedures, based on whether you have configured the node as a Junos Space node or as an FMPM node.

Adding a Junos Space Node to the Junos Space Fabric

To add a Junos Space node to the fabric:

1. On the Junos Space Platform UI, select **Administration > Fabric**.
The **Fabric** page appears.
2. Click the **Add Fabric Node** icon.
The **Add Node to Fabric** page appears.
3. Click the appropriate option button in the **Node Type** field to select the type of node you want to add.

NOTE: The options that are displayed depend on the number and type of nodes that are already part of the fabric.

Table 7 on page 143 describes the options that you can select while adding Junos Space nodes.

Table 7: Number of Existing Nodes and Permitted Node Types

Number of Nodes Existing in the Fabric	Permitted Node Types	Description
One	JBoss and DB Node DB Node Dedicated Cassandra Node	<p>When you add the second Junos Space node to the default single-node Junos Space fabric, you can add the new node as a JBoss and database node (standby load-balancer server), a dedicated Cassandra node, or the second and third nodes together as database nodes.</p> <p>In the case of database nodes, one node is designated the primary database node, and the other the secondary database node. The database VIP address must also be configured to enable database high availability.</p>
Two	JBoss Node DB Node Dedicated Cassandra Node	<p>When you add nodes to a two-node Junos Space fabric, Junos Space Platform allows you to add a JBoss node, a dedicated Cassandra node, or two nodes as database nodes.</p> <p>In the case of database nodes, one node is designated the primary database node, and the other the secondary database node. The database VIP address must also be configured to enable database high availability. If the Junos Space fabric already has one database node added, then you can add either a JBoss-only node or one database node as the secondary database node. The database node already existing in the fabric is the primary database node.</p>

Table 7: Number of Existing Nodes and Permitted Node Types (*continued*)

Number of Nodes Existing in the Fabric	Permitted Node Types	Description
Three or more—With one or no database node configured	JBoss Node DB Node Dedicated Cassandra Node	<p>When you add nodes to a Junos Space fabric with three or more nodes, with no database nodes added, Junos Space Platform allows you to add a JBoss node, a dedicated Cassandra node, or two nodes as database nodes.</p> <p>If the Junos Space fabric already has one database node added, then you can add a JBoss node, a dedicated Cassandra node, or one database node as the secondary database node. The database node already existing in the fabric is the primary database node.</p>
Three or more—With two database nodes configured	JBoss Node Dedicated Cassandra Node	<p>When you add nodes to a Junos Space fabric with three or more nodes, with two database nodes already configured, Junos Space Platform allows you to add either a JBoss node or a dedicated Cassandra node. You cannot add more than two database nodes to the fabric.</p>

NOTE: You can enable the Apache Cassandra service on any of the JBoss nodes added to the fabric to convert them to JBoss, Cassandra and database nodes or JBoss and Cassandra nodes. For more information about enabling the Cassandra service, see *Starting the Cassandra Service on a Junos Space Node*.

4. Perform one of the following procedures, based on the type of node you selected:
 - For the **JBoss and DB Node**, **JBoss Node**, and **Dedicated Cassandra Node** options, perform the following steps:
 - a. Enter a name for the node in the **Name** text box.
The name of the fabric node cannot exceed 32 characters and cannot contain spaces.
 - b. Enter the IP address of the node in the **IP address** field.
This is the IP address for the eth0 interface that you specified during the basic configuration of the appliance.
 - c. Enter the username in the **User** field.
 - d. Enter the password in the **Password** field.

NOTE: The login credentials that you specify in the User and Password fields must be the same username and password that you specified for SSH access using the Junos Space CLI during the initial installation and configuration of the node. If the credentials do not match, the node is not added.

- e. (Optional) Enter the fingerprint for the node in the **Fingerprint** field.

NOTE: To obtain the fingerprint of a node, see [“Obtaining Fingerprint of a Junos Space Node” on page 149](#).

- For the **DB Node** option, perform the following steps:
 - In the **Primary database** section:

NOTE: If you already have a database node as part of the fabric, the **Primary database** section does not appear. The existing database node is the primary database node and you can add only a secondary database node to the fabric.

- a. Enter a name for the primary database node in the **Name** text box.

The name of the fabric node cannot exceed 32 characters and cannot contain spaces.

- b. Enter the IP address of the primary database node in the **IP address** field.

This is the IP address for the eth0 interface that you specified during the basic configuration of the appliance.

- c. Enter the username in the **User** field.

- d. Enter the password in the **Password** field.

NOTE: The login credentials that you specify in the User and Password fields must be the same username and password that you specified for SSH access using the Junos Space CLI during the initial installation and configuration of the node. If the credentials do not match, the node is not added.

- e. (Optional) Enter the fingerprint for the node in the **Fingerprint** field..

NOTE: To obtain the fingerprint of a node, see [“Obtaining Fingerprint of a Junos Space Node” on page 149](#).

- f. Enter the VIP address for the database nodes in the **VIP** field.

The VIP address is used for communication between Junos Space nodes and database nodes. This IP address must be in the same subnet as the IP address assigned to the eth0 Ethernet interface, and the database VIP address must be different from the VIP address used to access the Web GUI and the FMPM nodes.

• In the **Secondary database** section:

- a. Enter a name for the secondary database node in the **Name** text box.

The name of the fabric node cannot exceed 32 characters and cannot contain spaces.

- b. Enter the IP address of the secondary database node in the **IP address** field.

This is the IP address for the eth0 interface that you specified during the basic configuration of the appliance.

- c. Enter the username in the **User** field.

- d. Enter the password in the **Password** field.

NOTE: The login credentials that you specify in the User and Password fields must be the same username and password that you specified for SSH access using the Junos Space CLI during the initial installation and configuration of the node. If the credentials do not match, the node is not added.

- e. (Optional) Enter the fingerprint for the node in the **Fingerprint** field..

NOTE: To obtain the fingerprint of a node, see [“Obtaining Fingerprint of a Junos Space Node” on page 149](#).

5. (Optional) Select the **Schedule at a later time** check box to specify a later date and time when you want the node to be added.

If you do not specify a date and time for adding the node, the node is added to the fabric when you complete this procedure and you click **Add** on the **Add Node to Fabric** page.

- a. Click the calendar icon and select the date.
- b. Click the arrow beside the time list and select the time.

NOTE: The selected time in the scheduler corresponds to the Junos Space server time but is mapped to the local time zone of the client computer.

6. Click **Add** to add the node to the fabric.

The **Job Information** dialog box appears, with a message indicating that the job to add the node is successfully scheduled. You can click the *job ID* link that is displayed in the dialog box to view job details. You can also navigate to the Job Management page to view job details.

7. Click **OK**.

You are returned to the **Fabric** page.

The node is added to the fabric and appears on the **Fabric** page. When you add a node, the node functions are automatically assigned by Junos Space Platform.

Adding an FMPM Node to the Junos Space Fabric

To add an FMPM node to the fabric:

1. On the Junos Space Platform UI, select **Administration > Fabric**.

The **Fabric** page appears.

2. Click the **Add Fabric Node** icon.

The **Add Node to Fabric** page appears.

3. Click the **Specialized Node** option button in the **Node Type** field to add an FMPM node.

4. Enter a name for the node in the **Name** text box.

The name of the fabric node cannot exceed 32 characters and cannot contain spaces.

5. Enter the IP address of the node in the **IP address** field.

NOTE: This is the IP address for the eth0 interface that you specified during the basic configuration of the appliance.

6. Enter the SSH username for the FMPM node in the **User** field.

7. Enter the password in the **Password** field.

The login credentials (SSH username and password) of the FMPM node that you specify in the **User** and **Password** fields must be the same username and password that you specified when you initially configured the node from the Junos Space CLI. If the credentials do not match, the node is not added.

8. (Optional) Enter the fingerprint for the node in the **Fingerprint** field.

NOTE: To obtain the fingerprint of a node, see [“Obtaining Fingerprint of a Junos Space Node” on page 149](#).

9. (Optional) Select the **Schedule at a later time** check box to specify a later date and time when you want the node to be added.

If you do not specify a date and time for the node to be added, the node is added to the fabric when you complete this procedure and you click **Add** on the **Add Node to Fabric** page.

- a. Click the calendar icon and select the date.
- b. Click the arrow beside the time list and select the time.

NOTE: The selected time in the scheduler corresponds to the Junos Space server time but is mapped to the local time zone of the client computer.

10. Click **Add** to add the node to the fabric.

The **Job Information** dialog box appears, with a message indicating that the job to add the node is successfully scheduled. You can click the *job ID* link that is displayed in the dialog box to view job details. You can also navigate to the Job Management page to view job details.

11. Click **OK**.

You are returned to the **Fabric** page.

The node is added to the fabric and appears on the **Fabric** page. When you add a node, the node functions are automatically assigned by Junos Space Platform.

Obtaining Fingerprint of a Junos Space Node

In a Junos Space cluster, the fingerprint of a node helps in authenticating and authorizing the node.

Starting from Junos Space Network Management Platform Release 17.1R1, the Fingerprint field is introduced to authenticate and authorize a node before adding the node to a Junos Space cluster.

To obtain the fingerprint of a Junos Space node:

1. Log in to access the command prompt of the node.

The Junos Space Settings menu appears.

2. Type **6** if the node is a JA2500 appliance or type **7** if the node is a Junos Space Virtual Appliance to access the shell.

You are prompted to enter the administrator password.

3. Enter the administrator password for the node..

The shell prompt appears.

4. Enter the **ssh-keygen -lf /etc/ssh/ssh_host_rsa_key -E md5** command as shown below to obtain the fingerprint of the node:

```
[root@space]# ssh-keygen -lf /etc/ssh/ssh_host_rsa_key -E md5
```

The node outputs its fingerprint as shown below:

```
2048 MD5:xx:xx:xx:00:00:00:0x:xx:x0:x0:00:00:x0:xx:00:x0:00
/etc/ssh/ssh_host_rsa_key.pub (RSA)
```

MD5:xx:xx:xx:00:00:00:0x:xx:x0:x0:00:00:x0:xx:00:x0:00 is the fingerprint in the MD5 format.

NOTE: Do not include MD5: when you enter fingerprint in the Fingerprint field while adding the node to a cluster.

Release History Table

Release	Description
17.1R1	Starting from Junos Space Network Management Platform Release 17.1R1, the Fingerprint field is introduced to authenticate and authorize a node before adding the node to a Junos Space cluster.

RELATED DOCUMENTATION

<i>Fabric Management Overview</i>
Viewing Nodes in the Fabric 150
<i>Dedicated Database Nodes in the Junos Space Fabric Overview</i>
<i>Overall System Condition and Fabric Load History Overview</i>
<i>Cassandra Nodes in the Junos Space Fabric Overview</i>

Viewing Nodes in the Fabric

IN THIS SECTION

- [Changing Views | 151](#)
- [Viewing Fabric Node Details | 151](#)

The Fabric Monitoring inventory page allows the administrator to monitor each node in the Junos Space fabric. You can also monitor the status of the database, load balancer, and application logic functions

running on each node, identify nodes that are overloaded or down, and view when the node was rebooted. The Fabric inventory page refreshes every 10 seconds, by default.

Changing Views

You can display fabric monitoring in tabular view. The fabric nodes appear in a table sorted by node name. Each fabric is a row in the Fabric Monitoring table.

To change views:

1. Select **Administration > Fabric**. The **Fabric** page appears.
2. Click a view indicator at the left of the title bar of the Fabric page.

Viewing Fabric Node Details

To view detailed runtime and status information for a node:

1. On the Junos Space Network Management Platform user interface, select **Administration > Fabric**.
The Fabric page that appears displays all the nodes in the Junos Space Platform fabric.
2. Right-click a node and select **View Fabric Node Details** or double-click inside a row corresponding to a node.

The **View Node Detail** pop-up window that appears displays three tabs: **Node Detail**, **Reboot Detail**, and **Process Detail**.

3. To view the node details, click the **Node Detail** tab.

[Table 8 on page 151](#) describes the details of the node.

Table 8: Information on the Node Detail Tab

Information	Description
Node name	Logical name assigned to the node NOTE: For the first node, Junos Space uses the node name that the user specifies during the initial configuration of the Junos Space Appliance (physical or virtual). For each subsequent node, the user must specify a node name when adding the node to the fabric.

Table 8: Information on the Node Detail Tab (*continued*)

Information	Description
Management IP (IPv4)	IPv4 address for the node
Management IP (IPv6)	IPv6 address for the node
Host Name	Host name of the node
Device Connection IP (IPv4)	IPv4 address for connecting to the device
Device Connection IP (IPv6)	IPv6 address for connecting to the device
Status	<p>Connection status for the node</p> <ul style="list-style-type: none"> • UP—Node is connected to the fabric • DOWN—Node is disconnected from the fabric
% CPU	<p>Percentage of CPU resource utilized by the node; from 0 to 100%</p> <ul style="list-style-type: none"> • Unknown—Percentage of CPU utilized is unknown, for example, because the node is not connected
% Memory	<p>Percentage of memory resource utilized by the node; from 0 to 100%</p> <ul style="list-style-type: none"> • Unknown—Percentage of memory utilized is unknown, for example, because the node is not connected
% SWAP	<p>Percentage of swap memory used</p> <ul style="list-style-type: none"> • Unknown—Percentage of SWAP memory utilized is unknown, for example, because the node is not connected
% DISK	<p>Percentage of the <code>/var</code> directory utilized by the node; from 0 to 100%</p> <ul style="list-style-type: none"> • Unknown—Percentage of the <code>/var</code> directory utilized by the node is unknown, for example, because the node is not connected

Table 8: Information on the Node Detail Tab (*continued*)

Information	Description
App Logic	<p>Application logic function status for the node</p> <ul style="list-style-type: none"> • UP—Application logic function is running on the node • DOWN—Application logic function enabled on the node but is not running • Unknown—Status for the application logic function is unknown, for example, because the node is not connected • N/A— Application logic function is not configured to run on the node • (Primary)—Configured primary Junos Space node in the fabric • FMPM (Primary)—The configured primary Fault Monitoring and Performance Monitoring (FMPM) node in the fabric • FMPM—The configured secondary FMPM node in the fabric • Deploying—Junos Space Platform and its applications are initializing after a recent JBoss restart • Parsing Schema—Device schema files are being parsed after a recent JBoss restart
Database	<p>Database function status for the node</p> <ul style="list-style-type: none"> • UP(Primary)—Database function is running on the node and the node is the primary database node • UP—Database function is running on the node In the case of dedicated database nodes, the secondary database node is always UP. • DOWN—Database function that is enabled on the node but is not running • Standby—Database function is on standby and could potentially transition to the UP state on failover • Unknown—Status for the database function is unknown, for example, because the node is not connected • N/A—Database function is not configured to run on the node <p>NOTE: By default, the database function is enabled on no more than two nodes in the fabric.</p>

Table 8: Information on the Node Detail Tab (*continued*)

Information	Description
Load balancer	<p>Load balancer function for the node</p> <ul style="list-style-type: none"> • UP—Load balancer function is running on the node • DOWN—Load balancer function that is enabled on the node is not running • Standby—Load balancer function is on standby and could potentially transition to the UP state on failover • Unknown—Status for the Load balancer function is unknown, for example, because the node might not be connected • N/A—Load balancer function is not running because it is not configured to run on the node <p>NOTE: By default, the Load balancer function is enabled on no more than two nodes in the fabric.</p> <ul style="list-style-type: none"> • (VIP)—Configured virtual IP node in the fabric
Hardware model	<p>Model of the Junos Space Appliance</p> <p>NOTE: The hardware model, which is applicable only to the hardware appliance, appears when you double-click a table row for a detailed view of the node.</p>
Software version	<p>Junos Space Network Management Platform release version</p> <p>NOTE: Software version appears when you double-click a table row for a detailed view of the node.</p>
Serial number	<p>The serial number for the Junos Space Appliance</p> <p>NOTE: Serial number appears when you double-click a table row for a detailed view of the node.</p>
Cluster Member IPs	IP addresses of the nodes in the fabric
Is Master Node	<p>Indicates whether the node is a primary node:</p> <ul style="list-style-type: none"> • TRUE—The node is a primary node • FALSE—The node is not a primary node
Is VIP Node	<p>Indicates whether the node is a virtual IP (VIP) node. The first (active) node and second (standby) node are VIP nodes.</p> <ul style="list-style-type: none"> • TRUE—The node is a VIP node. • FALSE—The node is not a VIP node.
Virtual Machine(s)	Lists the virtual machine IPs hosted by the node.

Table 8: Information on the Node Detail Tab (*continued*)

Information	Description
Host IP	IP address of the hosted virtual machine. This field is not applicable to Junos Space nodes and Fault Monitoring and Performance Monitoring (FMPM) nodes.

4. To view the details of the last reboot performed, select the **Reboot Detail** tab.

[Table 9 on page 155](#) lists the information related to the last reboot performed on this node.

Table 9: Information on the Reboot Detail Tab

Information	Description
Last Boot Time	Time at which the node was rebooted
Last Boot Reason	Reason why the node was rebooted
Last Rebooted By	Username of the user who rebooted the node

NOTE: If the node was rebooted from the CLI, or as a result of an upgrade or a fresh installation, the Last Rebooted By column displays **#system**.

[Table 10 on page 155](#) lists the default messages displayed to the user for different types of reboot actions.

Table 10: Default Messages for Different Reboot Actions

Reboot Action	Default Message
Rebooting after changing the network settings of the node from the Junos Space user interface	Reboot after Space Network Settings change
Upgrading Junos Space Platform	Space reboot after Software Upgrade
Rebooting from the CLI	Reboot from Shell/Other
Starting up Junos Space Platform for the first time	Junos Space startup after Installation/Software Upgrade

5. To view the details of the processes on this node, select the **Process Detail** tab.

Table 11 on page 156 lists the columns that specify the details of the following processes: JBoss, Apache Web Proxy, MySQL, OpenNMS, and PostgreSQL.

Table 11: Columns on the Process Detail Tab

Column Name	Description
Process	Name of the process
Status	Status of the process: UP, DOWN, STANDBY, or N/A
%CPU	Percentage of CPU resources used by the process on the node
%MEMORY	Percentage of memory used by the process on the node
Start Time	Time at which the process is initiated

NOTE: The status of the process and the percentage of CPU resources used by the process is queried once every 30 seconds.

Table 12 on page 156 lists the different statuses of the following processes: JBoss, Apache Web Proxy, MySQL, OpenNMS, PostgreSQL, and Cassandra.

Table 12: Process Status

Process Status	Description
UP	The process is up and active.
DOWN	The process is down and inactive.
STANDBY	The process is in standby mode and could potentially transition to the UP state on failover.
N/A	The process is never expected to be active on the node.

NOTE: If the MySQL database replication between nodes is broken, the MySQL process displays the status **OUT OF SYNC**. If the secondary database is in the process of receiving data and the primary database is still executing transactions then the status is **Syncing**. If the MySQL transactions are up-to-date between nodes, the MySQL process displays the status **UP**.

[Table 13 on page 157](#) describes the behavior and the expected status of the processes when OpenNMS is running on the Junos Space node.

Table 13: Status of the Processes When OpenNMS Is Running on the Junos Space Node

Process	Junos Space Node with OpenNMS		
	VIP Node	Secondary Node	Other Nodes
Apache Web Proxy	UP/DOWN	STANDBY	N/A
JBoss	UP/DOWN	UP/DOWN	UP/DOWN
MySQL	UP/DOWN	UP/DOWN	N/A
OpenNMS	UP/DOWN	STANDBY	N/A
PostgreSQL	UP/DOWN	UP/DOWN	N/A
Cassandra	UP/DOWN	UP/DOWN	UP/DOWN

[Table 14 on page 157](#) describes the behavior and the expected status of the processes when OpenNMS is running on the FMPM node.

Table 14: Status of the Processes When OpenNMS Is Running on the FMPM Node

Process	Junos Space Node			FMPM Node	
	VIP Node	Secondary Node	Other Nodes	OpenNMS VIP Node	OpenNMS Secondary Node
Apache Web Proxy	UP/DOWN	STANDBY	N/A	N/A	N/A
JBoss	UP/DOWN	UP/DOWN	UP/DOWN	N/A	N/A
MySQL	UP/DOWN	UP/DOWN	N/A	N/A	N/A
OpenNMS	N/A	N/A	N/A	UP/DOWN	STANDBY
PostgreSQL	N/A	N/A	N/A	UP/DOWN	UP/DOWN
Cassandra	UP/DOWN	UP/DOWN	UP/DOWN	N/A	N/A

NOTE: If an unexpected process is running on a node, the status of the process is shown as UP. If a node fails, the status of all processes on the node is shown as UNKNOWN.

For more information about modifying data on the Fabric inventory page, see *Junos Space User Interface Overview*.

RELATED DOCUMENTATION

<i>Overall System Condition and Fabric Load History Overview</i>
<i>Fabric Management Overview</i>
<i>Monitoring Nodes in the Fabric</i>
<i>Load-Balancing Devices Across Junos Space Nodes</i>
<i>Modifying the Network Settings of a Node in the Junos Space Fabric</i>