

Junos Space Network Management Platform

FIPS Evaluated Configuration Guide for Junos Space

Published
2021-02-18

Release
19.1R1

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 Network Management Platform FIPS Evaluated Configuration Guide for Junos Space
19.1R1

Copyright © 2021 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 | v

Documentation and Release Notes | v

Documentation Conventions | v

Documentation Feedback | viii

Requesting Technical Support | viii

Self-Help Online Tools and Resources | ix

Creating a Service Request with JTAC | ix

1

Overview

Understanding Junos Space in FIPS Mode | 11

About the Cryptographic Boundary on Junos Space | 11

How FIPS Mode Differs from Non-FIPS Mode | 12

Validated Version of Junos Space in FIPS Mode | 13

Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms | 13

FIPS Terminology | 13

Supported Cryptographic Algorithms | 14

Identifying Secure Product Delivery | 16

Understanding Management Interfaces | 17

2

Understanding Roles and Authentication Methods

Understanding Roles and Services for Junos Space in FIPS Mode | 19

Understanding Password Specifications and Guidelines for Junos Space in FIPS Mode | 42

Instructions for Validating the Junos Space Network Management Platform OVA and ISO Image | 43

3

Deploying the Junos Space Virtual Appliance

Junos Space Virtual Appliance Deployment Overview | 46

Deploying a Junos Space Virtual Appliance on a VMware ESXi Server | 47

Installing the VMware ESXi Server | 48

Installing a Junos Space Virtual Appliance on a VMware ESXi Server | 49

Installing a Junos Space Virtual Appliance by Using vSphere Client | 49

Installing a Junos Space Virtual Appliance by Using the OVF Tool | 50

Modifying RAM Settings for a Junos Space Virtual Appliance | 51

Adding Disk Resources for a Junos Space Virtual Appliance | 52

Starting Open VM Tools in Junos Space Platform | 54

Installing VI Toolkit for Perl on Junos Space Virtual Appliance | 55

4

Configuring the Junos Space Virtual Appliance

Configuring a Junos Space Virtual Appliance as a Junos Space Node | 59

Configuring a Junos Space Virtual Appliance | 60

Configuring Access to Junos Space Through a NAT Gateway | 70

Configuring the eth1 Ethernet Interface | 76

Installing Hot Patch | 77

5

Accessing Junos Space User Interface

Junos Space User Interface Overview in FIPS mode | 79

Junos Space Banner | 80

Task Tree | 81

Main Window | 83

Logging In to Junos Space UI in FIPS mode | 83

6

Zeroization

Zeroizing the System | 86

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | v
- Documentation Conventions | v
- Documentation Feedback | viii
- Requesting Technical Support | viii

Use this guide to operate Junos Space Hardware Appliances (JA2500), and Junos Space Virtual Appliances with Security Director and Network Director in Federal Information Processing Standards (FIPS) 140-2 Level 1 environment. FIPS 140-2 defines security levels for hardware and software that perform cryptographic functions.

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 vi 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 vi 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

Overview

Understanding Junos Space in FIPS Mode | 11

Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms | 13

Identifying Secure Product Delivery | 16

Understanding Management Interfaces | 17

Understanding Junos Space in FIPS Mode

IN THIS SECTION

- [About the Cryptographic Boundary on Junos Space | 11](#)
- [How FIPS Mode Differs from Non-FIPS Mode | 12](#)
- [Validated Version of Junos Space in FIPS Mode | 13](#)

Federal Information Processing Standards (FIPS) 140-2 defines security levels for hardware and software that perform cryptographic functions. By meeting the applicable overall requirements within the FIPS standard, Juniper Networks Junos Space Hardware Appliances (JA2500), and Junos Space Virtual Appliances with Security Director and Network Director complies with the FIPS 140-2 Level 1 standard.

Operating Junos Space in a FIPS 140-2 Level 1 environment requires enabling FIPS mode during the installation of Junos Space.

Junos Space administrators serve different functional roles. The CLI Admin User installs and configures Junos Space Appliances. A maintenance-mode administrator performs system-level tasks, such as troubleshooting and database restore operations. The *CLI Admin User* enables FIPS mode in Junos Space and sets up keys and passwords for the system.

For regulatory compliance information about FIPS for Juniper Networks products, see the [Juniper Networks Compliance Advisor](#).

About the Cryptographic Boundary on Junos Space

FIPS 140-2 compliance requires a defined *cryptographic boundary* around each *cryptographic module* on a device. Junos Space in FIPS mode prevents the cryptographic module from executing any software that is not part of the FIPS-certified distribution, and allows only FIPS-approved cryptographic algorithms to be used. No critical security parameters (CSPs), such as passwords and keys, can cross the cryptographic boundary of the module by, for example, being displayed on a console or written to an external log file.

Cryptographic boundary is determined by different configurations. For example, you can configure only Junos Space, Junos Space with Network Director, Junos Space with Security Director, or Junos Space with Security and Network Director.

How FIPS Mode Differs from Non-FIPS Mode

Unlike Junos Space in non-FIPS mode, Junos Space in FIPS mode is a *non-modifiable operational environment*. In addition, Junos Space in FIPS mode differs in the following ways from Junos Space in non-FIPS mode:

- Self-tests of all cryptographic algorithms are performed at startup.
- Self-tests of random number and key generation are performed continuously.
- Weak cryptographic algorithms such as Data Encryption Standard (DES) and Message Digest 5 (MD5) are disabled.
- Weak or unencrypted management connections must not be configured.
- Passwords must be encrypted with strong one-way algorithms that do not permit decryption.
- Administrator passwords must be at least 10 characters.
- The log in page displays *FIPS* after FIPS mode is enabled. [Figure 1 on page 12](#) displays FIPS mode is enabled.

Figure 1: Junos Space FIPS Mode Enabled



Validated Version of Junos Space in FIPS Mode

To determine whether a Network Director release is NIST-validated, see the compliance page on the Juniper Networks Web site (<https://apps.juniper.net/compliance/>).

Understanding FIPS Mode Terminology and Supported Cryptographic Algorithms

IN THIS SECTION

- [FIPS Terminology | 13](#)
- [Supported Cryptographic Algorithms | 14](#)

Use the definitions of FIPS terms and supported algorithms to help you understand Junos Space in FIPS mode.

FIPS Terminology

Critical security parameter (CSP)—Security-related information—for example, secret and private cryptographic keys and authentication data such as passwords and personal identification numbers (PINs)—whose disclosure or modification can compromise the security of a cryptographic module or the information it protects.

Cryptographic module—The set of software that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.

Super Administrator—Person with appropriate permissions who is responsible for securely enabling, configuring, monitoring, and maintaining Junos Space in FIPS mode. For details, see [“Understanding Roles and Services for Junos Space in FIPS Mode” on page 19](#).

FIPS—Federal Information Processing Standards. FIPS 140-2 specifies requirements for security and cryptographic modules. Junos Space in FIPS mode complies with FIPS 140-2 Level 1.

FIPS maintenance role—The role of the Super Administrator assumes to perform physical maintenance and or logical maintenance services, for example, hardware or software diagnostics. All plaintext secret, private keys, and unprotected CSPs are zeroized during the entry and exit of the maintenance role.

SSH—A protocol that uses strong authentication and encryption for remote access across a nonsecure network. SSH provides remote login, remote program execution, file copy, and other functions. It is intended as a secure replacement for **rlogin**, **rsh**, and **rcp** in a UNIX environment. To secure the information sent over administrative connections, use SSHv2 for CLI configuration. In Junos Space, SSHv2 is enabled by default, and SSHv1, which is not considered secure, is disabled.

Zeroization—Erasure of all CSPs and other user-created data. For details, see [“Zeroizing the System” on page 86](#).

Supported Cryptographic Algorithms

Each implementation of an algorithm is checked by a series of known answer test (KAT) self-tests. Any self-test failure results in a FIPS error state.

BEST PRACTICE: For FIPS 140-2 compliance, use only FIPS-approved cryptographic algorithms in FIPS mode.

The following cryptographic algorithms are supported in FIPS mode. Symmetric methods use the same key for encryption and decryption, while asymmetric methods use different keys for encryption and decryption.

AES—The Advanced Encryption Standard (AES), defined in FIPS PUB 197. The AES algorithm uses keys of 128, 192, or 256 bits to encrypt and decrypt data in blocks of 128 bits.

Diffie-Hellman—A method of key exchange across a nonsecure environment (such as the Internet). The Diffie-Hellman algorithm negotiates a session key without sending the key itself across the network by allowing each party to pick a partial key independently and send part of that key to the other. Each side then calculates a common key value. This is a symmetrical method—keys are typically used only for a short time, discarded, and regenerated.

ECDH—Elliptic Curve Diffie-Hellman. A variant of the Diffie-Hellman key exchange algorithm that uses cryptography based on the algebraic structure of elliptic curves over finite fields. ECDH allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel. The shared secret can be used either as a key or to derive another key for encrypting subsequent communications using a symmetric key cipher.

ECDSA—Elliptic Curve Digital Signature Algorithm. A variant of the Digital Signature Algorithm (DSA) that uses cryptography based on the algebraic structure of elliptic curves over finite fields. The bit size of the elliptic curve determines the difficulty of decrypting the key. The public key believed to be needed for ECDSA is about twice the size of the security level, in bits. ECDSA uses the P-256, P-384, and P-521 curves that can be configured under OpenSSH.

HMAC—Defined as “Keyed-Hashing for Message Authentication” in RFC 2104, HMAC combines hashing algorithms with cryptographic keys for message authentication. For Junos Space in FIPS mode, HMAC uses the iterated cryptographic hash functions SHA-1, SHA-256, and SHA-512 along with a secret key.

SHA-256, SHA-384, and SHA-512—Secure hash algorithms (SHA) belonging to the SHA-2 standard defined in FIPS PUB 180-2. Developed by NIST, SHA-256 produces a 256-bit hash digest, SHA-384 produces a 384-bit hash digest, and SHA-512 produces a 512-bit hash digest.

3DES (3des-cbc)—Encryption standard based on the original Data Encryption Standard (DES) from the 1970s that used a 56-bit key and was cracked in 1997. The more secure 3DES is DES enhanced with three multiple stages and effective key lengths of about 112 bits. For Junos Space in FIPS mode, 3DES is implemented with cipher block chaining (CBC).

The following [Table 3 on page 15](#) indicates supported algorithms for Junos Space:

Table 3: Supported Algorithms for Junos Space

Protocol	Key Exchange	Authentication	Encryption	MAC	Cipher
TLSv1.2	DH	RSA	AESGCM(128)	AEAD	DHE-RSA-AES128-GCM-SHA256
TLSv1.2	DH	RSA	AES(128)	SHA256	DHE-RSA-AES128-SHA256
TLSv1.2	DH	RSA	AESGCM(256)	AEAD	DHE-RSA-AES256-GCM-SHA384
TLSv1.2	DH	RSA	AES(256)	SHA256	DHE-RSA-AES256-SHA256
TLSv1.2	ECDH	RSA	AESGCM(128)	AEAD	ECDHE-RSA-AES128-GCM-SHA256
TLSv1.2	ECDH	RSA	AES(128)	SHA256	ECDHE-RSA-AES128-SHA256
TLSv1.2	ECDH	RSA	AESGCM(256)	AEAD	ECDHE-RSA-AES256-GCM-SHA384
TLSv1.2	ECDH	RSA	AES(256)	SHA384	ECDHE-RSA-AES256-SHA384

Junos Space supports the following third party cryptographic modules, which are FIPS compliance:

- Linux Kernel Crypto
- OpenSSL
- GnuTLS
- Libgcrypt
- Network Security Services
- JDK JCE
- Bouncy Castle

Identifying Secure Product Delivery

There are several mechanisms provided in the delivery process to ensure that a customer receives a product that has not been tampered with. The customer should perform the following checks upon receipt of a device to verify the integrity of the platform.

- Shipping label—Ensure that the shipping label correctly identifies the correct customer name and address as well as the device.
- Outside packaging—Inspect the outside shipping box and tape. Ensure that the shipping tape has not been cut or otherwise compromised. Ensure that the box has not been cut or damaged to allow access to the device.
- Inside packaging—Inspect the plastic bag and seal. Ensure that the bag is not cut or removed. Ensure that the seal remains intact.

If the customer identifies a problem during the inspection, he or she should immediately contact the supplier. Provide the order number, tracking number, and a description of the identified problem to the supplier.

Additionally, there are several checks that can be performed to ensure that the customer has received a box sent by Juniper Networks and not a different company masquerading as Juniper Networks. The customer should perform the following checks upon receipt of a device to verify the authenticity of the device:

- Verify that the device was ordered using a purchase order. Juniper Networks devices are never shipped without a purchase order.
- When a device is shipped, a shipment notification is sent to the e-mail address provided by the customer when the order is taken. Verify that this e-mail notification was received. Verify that the e-mail contains the following information:

- Purchase order number
 - Juniper Networks order number used to track the shipment
 - Carrier tracking number used to track the shipment
 - List of items shipped including serial numbers
 - Address and contacts of both the supplier and the customer
- Verify that the shipment was initiated by Juniper Networks. To verify that a shipment was initiated by Juniper Networks, you should perform the following tasks:
 - Compare the carrier tracking number of the Juniper Networks order number listed in the Juniper Networks shipping notification with the tracking number on the package received.
 - Log on to the Juniper Networks online customer support portal at <https://support.juniper.net/support/> to view the order status. Compare the carrier tracking number or the Juniper Networks order number listed in the Juniper Networks shipment notification with the tracking number on the package received.

Understanding Management Interfaces

The following management interfaces can be used in the evaluated configuration:

- Local Management Interfaces—Connect the RJ-45 to DB-9 serial port adapter to the serial port of the management device (laptop or PC) to access the Junos Space CLI. Connect one end of the Ethernet cable into the console port (labeled CONSOLE) on the front panel of the appliance and the other end of the Ethernet cable into the RJ-45 to DB-9 serial port adapter.

NOTE: If your laptop or PC does not have a DB-9 plug connector pin and you want to connect your laptop or PC directly to the appliance, use a combination of the RJ-45 to DB-9 socket adapter supplied with the appliance and a USB to DB-9 plug adapter. You must provide the USB to DB-9 plug adapter.

- Remote Management Protocols—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.

2

CHAPTER

Understanding Roles and Authentication Methods

Understanding Roles and Services for Junos Space in FIPS Mode | 19

Understanding Password Specifications and Guidelines for Junos Space in FIPS Mode | 42

Instructions for Validating the Junos Space Network Management Platform OVA and ISO Image | 43

Understanding Roles and Services for Junos Space in FIPS Mode

Junos Space Network Management Platform provides predefined roles that you can assign to users to define administrative responsibilities and specify the management tasks that a user can perform within applications and workspaces.

To assign roles to other users in Junos Space Network Management Platform, a user must be a Super Administrator or User Administrator.

Each predefined role defines a set of tasks for a single workspace, except the Super Administrator role, which defines all tasks for all workspaces. By default, Junos Space Network Management Platform provides read privileges on all objects associated with the task groups defined in a predefined role.

[Table 4 on page 19](#) and [Table 5 on page 34](#) show the Junos Space Network Management Platform predefined roles (A through Q and R through Z respectively) and corresponding tasks available for installed Junos Space applications.

The predefined roles that appear in the Junos Space Network Management Platform release that you are using depend on the Junos Space applications that you have installed. For the latest predefined roles, see **Network Management Platform > Role Based Access Control > Roles**.

For information about predefined roles for a specific Junos Space application, refer to the documentation for that Junos Space application.

Table 4: Predefined Roles (A through Q) for the Junos Space Network Management Platform

Predefined Role	Task Group and Tasks	Application > Workspace
Audit Log Administrator	Audit Log <ul style="list-style-type: none">• Archive/Purge Logs• Export Audit Logs	Network Management Platform > Audit Logs

Table 4: Predefined Roles (A through Q) for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
CLI Configlets Manager	CLI Configlets <ul style="list-style-type: none"> • Configlets <ul style="list-style-type: none"> • Create CLI Configlet • Delete CLI Configlets • Compare CLI Configlet Versions • View CLI Configlet Details • Modify CLI Configlet • Clone CLI Configlet • Apply CLI Configlet • Export Selected CLI Configlets • Export All CLI Configlets • Import CLI Configlet • Assign CLI Template to Domain 	Network Management Platform > CLI Configlets
CLI Configlets Manager	Devices <ul style="list-style-type: none"> • Device Management <ul style="list-style-type: none"> • Secure Console • Apply CLI Configlet 	Network Management Platform > Devices
CLI Configlets Operator	CLI Configlets <ul style="list-style-type: none"> • Configlets <ul style="list-style-type: none"> • Apply CLI Configlet 	Network Management Platform > CLI Configlets
CLI Configlets Operator	Devices <ul style="list-style-type: none"> • Device Management • Secure Console • Apply CLI Configlet 	Network Management Platform > Devices

Table 4: Predefined Roles (A through Q) for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Configuration File Manager	Configuration Files <ul style="list-style-type: none"> • Config Files Management <ul style="list-style-type: none"> • Backup Configuration Files • Delete Configuration Files • Restore Configuration Files • Compare Configuration File Versions • Export Configuration File • Modify Configuration File 	Network Management Platform > Configuration Files
Configuration Filter Manager	CLI Configlets <ul style="list-style-type: none"> • Configuration Filter <ul style="list-style-type: none"> • Create Configuration Filter • Modify Configuration Filter • Delete Configuration Filter • Assign Configuration Filter to Domain 	Network Management Platform > CLI Configlets
Configuration Filter Manager	Devices <ul style="list-style-type: none"> • Device Management <ul style="list-style-type: none"> • Device Configuration • Secure Console • Create/Edit/Delete Filter 	Network Management Platform > Devices
Configuration View Manager	CLI Configlets <ul style="list-style-type: none"> • Configuration View <ul style="list-style-type: none"> • Create Configuration View • Modify Configuration View • Delete Configuration View • View Configuration View Details • Export Configuration Views • Import Configuration Views 	Network Management Platform > CLI Configlets

Table 4: Predefined Roles (A through Q) for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Configuration View Manager	Devices <ul style="list-style-type: none"> • Device Management <ul style="list-style-type: none"> • Device Configuration <ul style="list-style-type: none"> • View Active Configuration • Secure Console 	Network Management Platform > Devices
Configuration View Operator	<ul style="list-style-type: none"> • CLI Configlets <ul style="list-style-type: none"> • Configuration View 	Network Management Platform > CLI Configlets
Configuration View Operator	<ul style="list-style-type: none"> • Devices <ul style="list-style-type: none"> • Device Management <ul style="list-style-type: none"> • Device Configuration <ul style="list-style-type: none"> • View Active Configuration • Secure Console 	Network Management Platform > Devices
Device Image Manager	Devices <ul style="list-style-type: none"> • Device Adapter <ul style="list-style-type: none"> • Add Adapter • Upgrade Adapter • Delete Adapter 	Network Management Platform > Devices
Device Image Manager	Images and Scripts <ul style="list-style-type: none"> • Images <ul style="list-style-type: none"> • Import Images • View Deployed Results • Modify Device Image • Delete Device Images • Stage Image on Device • MD5 Validation Result • Verify Image on Devices • Deploy Device Image • Undeploy JAM Package from Device • Remove Image from Staged Device • View Associated Devices • Assign Image to Domain 	Network Management Platform > Images and Scripts

Table 4: Predefined Roles (A through Q) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace
Device Images Read Only User	Images and Scripts <ul style="list-style-type: none">• Images<ul style="list-style-type: none">• View Deployed Results• View Associated Devices	Network Management Platform > Images and Scripts
Device Manager	CLI Configlets <ul style="list-style-type: none">• View CLI Configlet Details• Apply CLI Configlet	Network Management Platform > CLI Configlets

Table 4: Predefined Roles (A through Q) for the Junos Space Network Management Platform *(continued)*

Predefined Role	Task Group and Tasks	Application > Workspace
Device Manager		Network Management Platform > Devices

Table 4: Predefined Roles (A through Q) for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<p>Devices</p> <ul style="list-style-type: none"> • Device Management <ul style="list-style-type: none"> • Device Configuration <ul style="list-style-type: none"> • View Active Configuration <ul style="list-style-type: none"> • Create/Edit/Delete Filter • Resolve Out-of-band Changes • View/Assign Shared Objects • View Configuration Change Log • View Template Deployment • Modify Unmanaged Device Configuration • Review/Deploy Configuration <ul style="list-style-type: none"> • Validate on Device • Approve • Reject • Deploy • Modify Configuration • Assign Device to Domain • Device Inventory <ul style="list-style-type: none"> • Export Physical Inventory • View Associated Scripts • View License Inventory • View Logical Interfaces • View Physical Interfaces • View Physical Inventory • View Script Executions • View/Acknowledge Inventory Changes • View Software Inventory • View Staged Images <ul style="list-style-type: none"> • Delete Staged Images • Verify Checksum • Device Operations <ul style="list-style-type: none"> • Create LSYS • Manage Device Partition <ul style="list-style-type: none"> • Create Partition • Modify Partition 	

Table 4: Predefined Roles (A through Q) for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> • Delete Partition • Assign Partition to Domain • Delete Devices • Looking Glass <ul style="list-style-type: none"> • Export Looking Glass Results • Put in RMA State • Reactivate from RMA • Resynchronize with Network • Execute Scripts • Reboot Devices • Apply CLI Configlet • Clone Device • Activate Modeled Device • View/Download Configlet • Modify Serial Number • Device Access <ul style="list-style-type: none"> • Launch Device WebUI • Modify Authentication • Modify Device Target IP • Acknowledge Device Fingerprint • SSH to Device • Resolve Key Conflict • Manage Customized Attributes <ul style="list-style-type: none"> • Add Label • Delete Label • Upload Keys to Devices • Modify Serial Number • Secure Console • Modify Device Configuration • Device Discovery <ul style="list-style-type: none"> • Discover Targets • Specify Probes • Specify Credentials • Specify Fingerprints 	

Table 4: Predefined Roles (A through Q) for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> • Model Devices <ul style="list-style-type: none"> • Create Modeled Instance • Add More Devices • View Modeled Instance • View Modeled Device Status • View Configlet • Download Configlet • Delete Modeled Instances • Connection Profiles <ul style="list-style-type: none"> • Create Connection Profile • Modify Connection Profile • View Connection Profile • Delete Connection Profiles • Clone Connection Profile • Unmanaged Devices • View Alarms • View Performance Graphs • Device Discovery Profiles <ul style="list-style-type: none"> • Create Device Discovery Profile • Modify Device Discovery Profile • Clone Device Discovery Profile • Delete Device Discovery Profiles • Run Now Device Discovery Profile 	

Table 4: Predefined Roles (A through Q) for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Device Script Manager	<p>Images and Scripts</p> <ul style="list-style-type: none"> • Scripts <ul style="list-style-type: none"> • Compare Script Versions • Import Script • View Execution Results • Modify Script • Modify And Stage Scripts on Device • Delete Scripts • Stage Scripts on Devices • View Associated Devices • Verify Scripts on Devices • Verification Results • Enable Scripts on Devices • Disable Scripts on Devices • Remove Scripts from Devices • Execute Script on Devices • Export Scripts • Modify Scripts Type • Assign Script to Domain • Script Bundles <ul style="list-style-type: none"> • Create Script Bundle • Embedded Script • Modify Script Bundle • Delete Script Bundles • Stage Script Bundle on Devices • View Associated Devices • Enable Script Bundle on Devices • Disable Script Bundle on Devices • Execute Script Bundle on Devices 	Network Management Platform > Images and Scripts
Device Script Operator	<p>Devices</p> <ul style="list-style-type: none"> • Device Management • Secure Console 	Network Management Platform > Devices

Table 4: Predefined Roles (A through Q) for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Device Script Operator	Images and Scripts <ul style="list-style-type: none"> • Scripts <ul style="list-style-type: none"> • Compare Script Versions • Execute Script on Devices 	Network Management Platform > Images and Scripts
Device Script Read Only User	Images and Scripts <ul style="list-style-type: none"> • Scripts <ul style="list-style-type: none"> • Compare Script Versions • View Execution Results • View Associated Devices • Export Scripts • Script Bundles 	Network Management Platform > Images and Scripts
Domain Administrator	Devices <ul style="list-style-type: none"> • Device Management • Secure Console 	Network Management Platform > Devices
Domain Administrator	Role Based Access Control <ul style="list-style-type: none"> • Domains <ul style="list-style-type: none"> • Create Domain • Modify Domain • Delete Domain • Export Domain • Assign Devices to Domain • Assign Domain to Users • User Accounts 	Network Management Platform > Role Based Access Control

Table 4: Predefined Roles (A through Q) for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
FMPM Manager	Network Monitoring <ul style="list-style-type: none"> • Node List <ul style="list-style-type: none"> • Resync Nodes • Search • Outages • Dashboard • Events • Alarms • Notifications • Assets • Reports • Charts • Topology • Admin 	Network Management Platform > Network Monitoring
FMPM Read Only User	Network Monitoring <ul style="list-style-type: none"> • Node List <ul style="list-style-type: none"> • Resync Nodes • Search • Outages • Dashboard • Events • Alarms • Notifications • Assets • Reports • Charts • Topology 	Network Management Platform > Network Monitoring

Table 4: Predefined Roles (A through Q) for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Job Administrator	Jobs <ul style="list-style-type: none"> • Job Management <ul style="list-style-type: none"> • Cancel My Job <ul style="list-style-type: none"> • Cancel Any Job • Reassign Jobs • Archive/Purge Jobs • Reschedule Job • View Recurrence 	Network Management Platform > Jobs
Job User	Jobs <ul style="list-style-type: none"> • Job Management <ul style="list-style-type: none"> • Cancel My Job • Reschedule Job • View Recurrence 	Network Management Platform > Jobs
Operation Manager	Devices <ul style="list-style-type: none"> • Device Adapter <ul style="list-style-type: none"> • Add Adapter • Upgrade Adapter • Delete Adapter 	Network Management Platform > Devices

Table 4: Predefined Roles (A through Q) for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Operation Manager		Network Management Platform > Images and Scripts

Table 4: Predefined Roles (A through Q) for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<p>Images and Scripts</p> <ul style="list-style-type: none"> • Images <ul style="list-style-type: none"> • Import Images • View Deployed Results • Modify Device Image • Delete Device Images • Stage Image on Device • MD5 Validation Result • Verify Image on Devices • Deploy Device Image • Remove Image from Staged Device • View Associated Devices • Assign Image to Domain • Scripts <ul style="list-style-type: none"> • Compare Script Versions • Import Script • View Execution Results • Modify Script • Modify And Stage Scripts on Device • Delete Scripts • Stage Scripts on Devices • View Associated Devices • Verify Scripts on Devices • Verification Results • Enable Scripts on Devices • Disable Scripts on Devices • Remove Scripts from Devices • Execute Script on Devices • Export Scripts • Modify Scripts Type • Assign Script to Domain • Script Bundles <ul style="list-style-type: none"> • Create Script Bundle • Embedded Script 	

Table 4: Predefined Roles (A through Q) for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> • Modify Script Bundle • View Associated Devices • Enable Script Bundle on Devices • Disable Script Bundle on Devices • Delete Script Bundles • Stage Script Bundle on Devices • Execute Script Bundle on Devices • Assign Script Bundle to Domain • Operations <ul style="list-style-type: none"> • Create Operation • Clone Operation • Modify Operation • Delete Operations • Import Operations • Export Operations • Run Operation • View Operation Results • Assign Operation to Domain 	

Table 5: Predefined Roles (R through Z) for the Junos Space Network Management Platform

Predefined Role	Task Group and Tasks	Application > Workspace
Report Administrator	Reports <ul style="list-style-type: none"> • Generated Reports <ul style="list-style-type: none"> • Delete Generated Report • View Generated Report 	Network Management Platform > Reports

Table 5: Predefined Roles (R through Z) for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Report Definition Administrator	<p>Reports</p> <ul style="list-style-type: none"> • Report Definitions <ul style="list-style-type: none"> • Create Report Definition • Modify Report Definition • Delete Report Definition • Clone Report Definition • View Report Definition • Generate Report • Assign Report Definition to Domain 	Network Management Platform > Reports
Super Administrator	Manages all Junos Space Network Management Platform task groups and tasks. See Network Management Platform > Users > Roles > Super Administrator > View Detail for a list of tasks that are currently supported.	All Junos Space Network Management Platform workspaces

Table 5: Predefined Roles (R through Z) for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
System Administrator		Network Management Platform > Administration

Table 5: Predefined Roles (R through Z) for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<p>Administration</p> <ul style="list-style-type: none"> • Fabric <ul style="list-style-type: none"> • Extended Periods of High CPU • List of HPROF Files • Large Database Tables • Last JBoss Restarted Time • Device Management Sessions • Add Fabric Node • Delete Fabric Node • View Fabric Node Alarms • Device Load Balancing • Shutdown/Reboot Node(s) • Space Node Settings • SNMP Configuration • SNMP Manager • NAT Configuration • Check For File Integrity • Reset MySQL Replication • SNMP Start • SNMP Stop • SNMP Restart • System Snapshot • Generate Key • Database Backup and Restore <ul style="list-style-type: none"> • Database Backup • Delete Backup • Restore • Restore From Remote File • Space Troubleshooting <ul style="list-style-type: none"> • Log Configuration • Applications <ul style="list-style-type: none"> • Modify Application Settings • Refresh Search Index 	

Table 5: Predefined Roles (R through Z) for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> • Manage Services • Uninstall Application • Upgrade Application • Add Application • Upgrade Platform • Licenses <ul style="list-style-type: none"> • Import License • Tags <ul style="list-style-type: none"> • Create Public Tag • Modify Public Tag • Delete Public Tags • Delete Private Tags • Make Tag Public • Mark as Favorite • Unmark as Favorite • Export Tags • Filter Management <ul style="list-style-type: none"> • Save Filter • Modify Filter • Delete Filter • DMI Schemas <ul style="list-style-type: none"> • Set as Default Schema • View Missing Schemas • View/Delete Unused Schemas <ul style="list-style-type: none"> • Delete Unused Schemas • Update Schema • Authentication Servers • Platform Certificate • CA/CRL Certificates • SMTP Servers 	

Table 5: Predefined Roles (R through Z) for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> • Audit Log Forwarding <ul style="list-style-type: none"> • Create Audit Log Forwarding Criterion • Modify Audit Log Forwarding Criterion • Delete Audit Log Forwarding Criterion • Enable Audit Log Forwarding Criterion • Email Listeners • Proxy Server • Purging Policy <ul style="list-style-type: none"> • Modify Purging Policy • Edit Purging Policy • Set Policy Status 	
Tag Administrator	<ul style="list-style-type: none"> • Tags <ul style="list-style-type: none"> • Modify Public Tag • Delete Public Tags • Delete Private Tags • Mark as Favorite • Unmark as Favorite • Export Tags • Make Tag Public • Create Public Tag 	Network Management Platform > Administration > Tags
Template Design Manager	<ul style="list-style-type: none"> • Device Templates <ul style="list-style-type: none"> • Definitions <ul style="list-style-type: none"> • Create Template Definition • Manage CSV Files • Modify Template Definition • Clone Template Definition • Publish Template Definition • Unpublish Template Definition • Delete Template Definition • Export Template Definition • Import Template Definition • Assign Definition to Domain 	Network Management Platform > Device Templates > Definitions

Table 5: Predefined Roles (R through Z) for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Template Manager	<ul style="list-style-type: none"> • Devices <ul style="list-style-type: none"> • Create Quick Template • Device Templates <ul style="list-style-type: none"> • Templates <ul style="list-style-type: none"> • Create Quick Template • Create Template from Definition • View Template Details • Modify Quick Template • Modify Template • Delete Template • Audit Template Configuration • Compare Template Against Device • Clone Template • Undeploy Template • View Template Association • Export Quick Template • Import Quick Template • Assign/Deploy Template <ul style="list-style-type: none"> • Assign Template • Deploy Template • Assign Template to Domain • Unassign from Device • Manage CSV Files 	<p>Network Management Platform > Devices</p> <p>Network Management Platform > Device Templates > Templates</p>

Table 5: Predefined Roles (R through Z) for the Junos Space Network Management Platform (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
User Administrator	<ul style="list-style-type: none"> • Role Based Access Control <ul style="list-style-type: none"> • User Accounts <ul style="list-style-type: none"> • Create User • Modify User • Delete Users • Disable Users • Enable Users • Unlock Users • Clear Local Passwords • Roles <ul style="list-style-type: none"> • Create Role • Modify Role • Clone Role • Delete Roles • Export Roles • Import Roles • Remote Profiles <ul style="list-style-type: none"> • Create Remote Profile • Modify Remote Profile • Delete Remote Profiles • API Access Profiles <ul style="list-style-type: none"> • View API Access Profile Detail • Create API Access Profile • Modify API Access Profile • Delete API Access Profiles • User Sessions <ul style="list-style-type: none"> • Terminate User Session 	Network Management Platform > Role Based Access Control
Xpath and Regex Manager	<ul style="list-style-type: none"> • CLI Configlets <ul style="list-style-type: none"> • Xpath and Regex <ul style="list-style-type: none"> • Create Xpath / Regex • Modify Xpath / Regex • Delete Xpath / Regex • Assign XPath / Regex to Domain 	Network Management Platform > CLI Configlets

Understanding Password Specifications and Guidelines for Junos Space in FIPS Mode

Ensure that the device is in FIPS mode before you configure the Super Administrator or any users. All passwords established for users by the Super Administrator must conform to the following Junos Space in FIPS mode requirements. Attempts to configure passwords that do not conform to the following specifications result in an error.

- **Length.** Passwords must contain between 10 and 20 characters.
- **Character set requirements.** Passwords must contain at least three of the following five defined character sets:
 - Uppercase letters
 - Lowercase letters
 - Digits
 - Keyboard characters not included in the other four sets—such as the percent sign (%) and the ampersand (&)
- **Authentication requirements.** All passwords and keys used to authenticate peers must contain at least 10 characters, and in some cases the number of characters must match the digest size—for example, 20 characters for SHA-1 authentication.

Guidelines for strong passwords. Strong, reusable passwords can be based on letters from a favorite phrase or word and then concatenated with other unrelated words, along with added digits. In general, a strong password is:

- Easy to remember so that users are not tempted to write it down.
- Made up of mixed alphanumeric characters and punctuation. For FIPS compliance include at least one change of case, one or more digits, and one or more punctuation marks.
- Changed periodically.
- Not divulged to anyone.

Characteristics of weak passwords. Do not use the following weak passwords:

- Words that might be found in or exist as a permuted form in a system files such as `/etc/passwd`.
- The hostname of the system (always a first guess).
- Any word or phrase that appears in a dictionary or other well-known source, including dictionaries and thesauruses in languages other than English; works by classical or popular writers; or common words and phrases from sports, sayings, movies or television shows.

- Permutations on any of the above—for example, a dictionary word with letters replaced with digits (**root**) or with digits added to the end.
- Any machine-generated password. Algorithms reduce the search space of password-guessing programs and so must not be used.

Instructions for Validating the Junos Space Network Management Platform OVA and ISO Image

To check the credibility of JA2500 or any virtual application image, compare the checksum values. Verifying the checksum helps to validate that the device image is staged properly and is not corrupted or altered in any way.

To view the checksum on your device, use the following procedure:

1. Using a Web browser, navigate to <https://support.juniper.net/support/downloads/>.
2. Enter a product name in the text box. For example, Junos Space Network Management Platform.
3. Select a version from the drop-down list. For example, 19.1.
4. Download the **ova** and **iso** image to your computer.
5. From the shell prompt, enter the following commands to view the checksum values.

```
>md5sum space-19.1R1.391861.ova
```

```
ff6a46ee6c81644babb4dd7e5e98dd03 space-19.1R1.391861.ova
```

```
>sha1sum space-19.1R1.391861.ova
```

```
9ee92099ec45788366853b8d167afe6efab29b4d space-19.1R1.391861.ova
```

```
>sha256sum space-19.1R1.391861.ova
```

```
2f0ddd61f502d92154d5714ac76916df0b7dbf4b7d71b6088f5304e8f865b535
space-19.1R1.391861.ova
```

```
>sha512sum space-19.1R1.391861.ova
```

```
85cd773ad4e4781d3765410dd9230bc913181715916db20fc042c07fb404339
67e6388e7c14d5df0139cb9b212a7446fc037e0c06097a217eb95a220bc4c2822
space-19.1R1.391861.ova
t
```

```
>md5sum space-19.1R1.391861-usb.iso
```

```
d26baf9692eda6ded34e6039b30b53a2 space-19.1R1.391861-usb.iso
```

```
>sha1sum space-19.1R1.391861-usb.iso
```

```
6a56d806b5a1dc082b04394b8d9db13a1c53028d space-19.1R1.391861-usb.iso
```

```
>sha256sum space-19.1R1.391861-usb.iso
```

```
4c487bbadfd19304058a2c2307192643b3c0f8512684e7c4ca5a1b2b31058869
space-19.1R1.391861-usb.iso
```

```
>sha512sum space-19.1R1.391861-usb.iso
```

```
e04ee4ba6298c9d7bea7cb213a158b9bc7e78316a01a5fcb6d24188ad91ef41
3d3110e919a81c8ed54db23b304e87ee085a6b4283a90ea767f7931a9c1faa726
space-19.1R1.391861-usb.iso
```

To view the checksum on the download page, use the following procedure:

1. Using a Web browser, navigate to <https://support.juniper.net/support/downloads/>.
2. Enter a product name in the text box. For example, Junos Space Network Management Platform.
3. Select a version from the drop-down list. For example, 19.1.
4. Click the **Checksums** option. A pop-up window displays the checksum values.

Compare the checksum values between the download site and the downloaded image. If the checksum values are the same, then the image is a valid image, and you can use the image for installing and upgrading. If the checksum values are different, then the image is damaged, partially downloaded, or manually modified.

3

CHAPTER

Deploying the Junos Space Virtual Appliance

Junos Space Virtual Appliance Deployment Overview | 46

Deploying a Junos Space Virtual Appliance on a VMware ESXi Server | 47

Starting Open VM Tools in Junos Space Platform | 54

Installing VI Toolkit for Perl on Junos Space Virtual Appliance | 55

Junos Space Virtual Appliance Deployment Overview

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

You can deploy the Junos Space Virtual Appliance *.ova file on a VMware ESX server version 6.5 or later or VMware ESXi server version 6.5 or later.

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 and configure the Junos Space Virtual Appliance.

NOTE: Where the Junos Space Virtual Appliance documentation references “ESX server,” you can use either the VMware ESX server version 6.5 or later or VMware ESXi server Version 6.5 or later.

NOTE: VMware VMotion is not supported for moving Junos Space Virtual Appliances from one VMware ESX server to another VMware ESX server.

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.

- 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 54 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.
- VMware VMotion is not supported for moving Junos Space Virtual Appliances from one VMware ESX server to another VMware ESX server.

Deploying a Junos Space Virtual Appliance on a VMware ESXi Server

The Junos Space Virtual Appliance requires a VMware ESXi server 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 not 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 46](#).

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 | 48](#)
2. [Installing a Junos Space Virtual Appliance on a VMware ESXi Server | 49](#)
3. [Modifying RAM Settings for a Junos Space Virtual Appliance | 51](#)
4. [Adding Disk Resources for a Junos Space Virtual Appliance | 52](#)

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 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 | 49
- Installing a Junos Space Virtual Appliance by Using the OVF Tool | 50

You can use vSphere Client 6.5 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 6.5:

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-19.1R1.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

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.
- 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.

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 52](#) 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
<code>/var</code>	MySQL database, PostgreSQL database, database backup file, and disaster recovery data files	FMPM data, MySQL database, PostgreSQL database
<code>/var/log</code>	All system log files	All system log files
<code>/tmp</code>	Temporary files	Temporary files
<code>/</code>	Worldwide adapters, JBoss configuration files	OpenNMS installation

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 59.

Starting Open VM Tools in Junos Space Platform

Junos Space Network Management Platform supports the use of Open VM Tools to facilitate better management and the seamless interaction of the VMware ESXi 6.5 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 10.0.5 on the Junos Space Virtual Appliance.

To download utilities and drivers necessary to build Open VM Tools, see <https://sourceforge.net/projects/open-vm-tools/files/open-vm-tools/stable-10.0.x/open-vm-tools-10.0.5-3227872.tar.gz/download>. For more information about building Open VM Tools, see <https://github.com/vmware/open-vm-tools#building-open-vm-tools>.

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.

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](#).

4

CHAPTER

Configuring the Junos Space Virtual Appliance

Configuring a Junos Space Virtual Appliance as a Junos Space Node | 59

Installing Hot Patch | 77

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.

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 task:

- [Configuring a Junos Space Virtual Appliance | 60](#)
- [Configuring Access to Junos Space Through a NAT Gateway | 70](#)
- [Configuring the eth1 Ethernet Interface | 76](#)

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
```

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 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. 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.

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

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

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

- f. 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:
```

- g. Retype the password for cluster maintenance mode and press Enter.
- h. You are prompted to specify whether you want to enable FIPS mode of Junos Space installation or not.

```
Do you want to enable FIPS mode of Space installation? [y/N]
```

- Type **y** to enable FIPS mode.

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

```
Settings Summary:
```

```
> IP Change: eth0 is 10.204.97.165 / 255.255.240.0
> Default Gateway - 10.204.111.254 on eth0
> DNS add: 10.209.194.50
> Create as first node or standalone
> Web IP address is 10.204.98.59
> NTP add: device1.example.com
> Node display name is "jsnodel"
> Password for Junos Space maintenance mode is set.
```

```

> FIPS mode is enabled
A> Apply settings
C> Change settings
Q> Quit and set up later
R> Redraw Menu
.
.
.
FIPS mode enabled successfully.
Node will be rebooted in 2 minutes

```

The configuration of the Junos Space Virtual Appliance in FIPS mode 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.

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.

Configuring Access to Junos Space Through a NAT Gateway

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 [d](#).

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.

Installing Hot Patch

Junos Space hot patches are signed using SHA256 and it should be installed using a script. The script validates the signature of the hot patch and triggers hot patch execution.

Run the following script to install the hot patch:

```
/var/www/cgi-bin/installHotpatch.sh -f <HOTPATCH_FILE> [-patch-script  
<HOT_PATCH_SCRIPT>] [ARGUMENTS_TO_HOTPATCH_SCRIPT]
```

5

CHAPTER

Accessing Junos Space User Interface

Junos Space User Interface Overview in FIPS mode | **79**

Logging In to Junos Space UI in FIPS mode | **83**

Junos Space User Interface Overview in FIPS mode

IN THIS SECTION

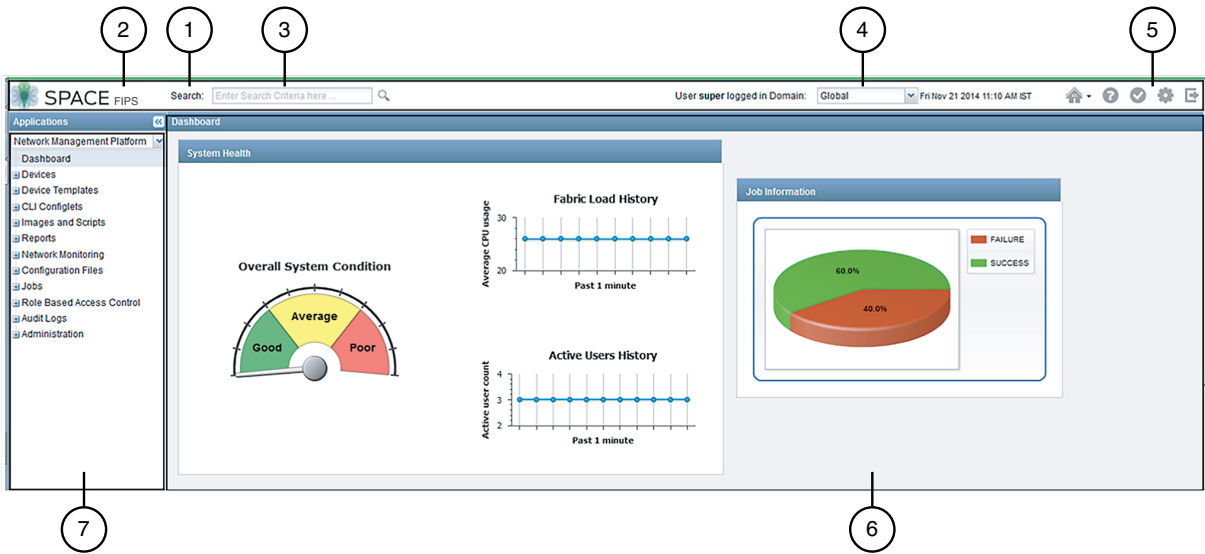
- [Junos Space Banner | 80](#)
- [Task Tree | 81](#)
- [Main Window | 83](#)

The Junos Space UI in FIPS mode is designed to look and behave in a way that most users are familiar with. The left tree structure facilitates navigation and the right pane displays information about the workspace or task selected in the left pane. Multiple users can access the UI through Web browsers concurrently. All users have access to the same current information in the same system wide database. Access to tasks and objects is controlled by permissions assigned to each user.

The Junos Space UI in FIPS mode is common to Junos Space Network Management Platform and Junos Space applications. The information displayed on the Junos Space UI changes according to the application you select. The examples shown here are from the Junos Space Platform UI. Other applications may have design variations.

When you log in to Junos Space Platform after you enable FIPS mode, the previously configured home page is displayed. The Junos Space Platform Dashboard, which is the default home page, is shown in [Figure 2 on page 80](#).

Figure 2: Junos Space Platform Default Home Page



1—Junos Space Banner	5—Global Action Icons
2—FIPS Mode	6—Junos Space Dashboard
3—Global Search Text Box	7—Task Tree
4—Domain Switcher	

This display contains three main parts: a task tree on the left, which is always available; a main window on the right, whose content changes as you select items from the task tree; and a banner across the top, which offers the date and time, the domain to which you are logged in, global search, and several icon buttons for frequently used actions. These parts are described in the following sections.






Junos Space Banner

The Junos Space banner, as indicated in [Figure 2 on page 80](#), displays the date and server time in the active time zone, the domain to which you are logged in, global search, and the global actions icons. This banner is always present.

NOTE: If you access the Junos Space Platform UI in two tabs of the same browser with two different domains selected and access the same page in both tabs, the information displayed on the page is based on the latest domain selected. To view pages that are accessible only in the Global domain, ensure that you are in the Global domain in the most recent tab in which you are accessing the UI.

[Table 7 on page 81](#) describes the global action icons on the right side of the banner.

Table 7: Global Action Icons

Global Action Icon	Description
	Enables you to access the Junos Space home page or set the Junos Space home page.
	Displays the application Help. To access workspace context-sensitive Help, click the Help icon after navigating to that workspace.
	Displays the My Jobs dialog box from which you can view the progress and status of your current managed jobs. You can view all your completed, in-progress, canceled, and scheduled jobs in Junos Space Platform.
	Displays the Change User Settings dialog box from which you can change user preferences, such as the password.
	Logs you out of the system.

Task Tree

The task tree on the left side of the display is always present and facilitates navigation in the Junos Space Platform UI. As shown in [Figure 2 on page 80](#), when you first log in, the Application Selector list displays Network Management Platform by default. You can drop this list down to see all the Junos Space applications available on your system.

You can collapse the task tree to the left by clicking the double left arrow buttons in its header, and reexpand it by clicking the double right arrow buttons.

Below the application name is the word **Dashboard**, selected by default. It indicates that what you see in the right-hand window is the dashboard for the current application—in this case, Junos Space Platform. The dashboard shows several measures of overall system health.

Below the Dashboard item in the tree is a list of the workspaces available in the current application. This list forms the top level of the task tree. If you select a different application from the **Applications** list, you see the workspace list change. This topic describes the workspaces for Junos Space Platform; for the workspaces in other applications, see the documentation for those applications.

The workspaces in the Junos Space Platform are described at a high level in [Table 8 on page 82](#).

Table 8: Workspace Names

Workspace Name	Function
Devices	Manage devices, including adding, discovering, importing, and updating them.
Device Templates	Create configuration definitions and templates used to deploy configuration changes on multiple Juniper Networks devices.
CLI Configlets	Easily apply a configuration to a device. Configlets are configuration tools provided by Junos OS.
Images and Scripts	Deploy, verify, enable, disable, remove, and execute scripts deployed to devices. Download a device image from the Juniper Networks Software download site to your local file system, upload it into Junos Space, and deploy it on one or more devices simultaneously.
Reports	Generate customized reports for managing network resources.
Network Monitoring	Assess the performance of your network, not only at a point in time, but also over a period of time.
Configuration Files	See Managing Configuration Files Overview .
Jobs	Monitor the progress of ongoing jobs.
Role Based Access Control	Add, manage, and delete users, custom roles, domains, and remote profiles. From this workspace, you can also manage user sessions.
Audit Logs	View and filter system audit logs, including those for user login and logout, tracking device-management tasks, and displaying services that were provisioned on devices.
Administration	Add network nodes, back up your database, manage licenses and applications, or troubleshoot.

You can expand any of these workspaces by clicking the expansion symbol (+) to the left of its name. When you do so, the next level of the task tree for that workspace opens. Some items at this second level may also be expandable subgroups.

You can expand as many workspaces or task groups as you like; previously expanded ones remain open until you collapse them. The design of the task tree enables you to jump from area to area within an application with the minimum number of selections.

Main Window

When you log in to Junos Space Platform, the main window shows the application dashboard by default. If you have set another home page, the main window displays that page.

When you select a workspace name (as opposed to expanding it), the main window changes and displays graphical statistics for that workspace. This display is called *Workspace Statistics*. It is similar in functionality to the overall system dashboard, but it pertains only to that workspace.

Selecting the name of a task group or task within the workspace causes the main window to display an inventory of the objects managed in tabular format.

Logging In to Junos Space UI in FIPS mode

You can connect to the Junos[®] Space UI by using your Web browser. The minimum browser requirements supported by Junos Space Network Management Platform are Internet Explorer version 11, Google Chrome version 22, and Mozilla Firefox version 45.

We recommend a screen resolution of 1280 x 1024 pixels or higher.



WARNING: To avoid a Browser Exploit Against SSL/TLS (BEAST) attack, whenever you log in to Junos Space through a browser tab or window, make sure that the tab or window was not previously used to access a non-HTTPS website. Best practice is to close your browser and relaunch it before logging in to Junos Space.

NOTE:

- The Network Monitoring Topology feature of Junos Space Platform is not supported on Internet Explorer.
- Before you log in to Junos Space, ensure that the Adobe Flash version 10 or later plug-in is installed in your browser.

To access and log in to Junos Space UI in FIPS mode:

1. In the address bar of your browser window, enter **<https://virtual-IP-address/mainui/>**, where *virtual-IP-address* is the previously configured virtual IP (VIP) address that is used for Web access to Junos Space.
2. Press Enter or click **Search**.

The Junos Space login page appears.
3. In the **Username** text box, enter your username. The default username is **super**. For information about how to change your username, consult your system administrator.
4. In the **Password** text box, enter your password. For information about how to change your password, see https://www.juniper.net/documentation/en_US/junos-space18.4/platform/topics/task/configuration/junos-space-user-password-changing.html
5. (Optional) If the remote authentication server is configured for Challenge/Response, you are presented with challenge questions. Provide valid responses to the challenge questions to log in successfully.
6. Click **Log In**.

The Junos Space FIPS mode home page appears. If the home page is not set, the Junos Space Dashboard page is displayed. If the home page is inaccessible due to role or domain restrictions, a warning message is displayed and the Junos Space Dashboard page is loaded.

NOTE: If you are a user with access to more than one domain, then an informational message about switching domains is displayed in a dialog box.

Do one of the following:

- To prevent the informational message from appearing again, ensure that the **Don't show again** check box is selected and click **OK**. The **Don't show again** check box is selected by default.
- To allow the informational message to continue appearing, clear the **Don't show again** check box and click **OK**.

NOTE: By default, Junos Space Platform authenticates a user's username and password. However, you can also use certificate-based authentication to authenticate and authorize sessions among various servers and users. To configure certificate-based authentication, see https://www.juniper.net/documentation/en_US/junos-space18.4/platform/topics/concept/junos-space-certificate-management.html

6

CHAPTER

Zeroization

Zeroizing the System | 86

Zeroizing the System

For FIPS 140-2 compliance, you must zeroize the system to remove sensitive information before disabling FIPS mode on the device.

As a CLI Admin User, you select the **Zeroize CSP** option to remove all user-created files from a device and replace the user data with zeros. This command completely erases the following CSPs:

- Space CA certificate key
- Certificate Keys of following services:
 - httpd(default and user uploaded)
 - NMA
 - MySQL
 - PostgreSQL
 - JBoss
 - Csync
 - Cassandra
 - OpenNMS
- Java Keystore
- /etc/sysconfig/JunosSpace/pwd
- DR device credentials file
- DR SSH credentials file
- Linux SMTP config file
- OpenNMS SMTP config file
- OpenNMS users credential file
- SNMP config files(Space and OpenNMS)
- Device SNMP details files in Opennms
- SSH host keys
- SSH Host key for node communication
- Junos Space SSH Host key for device communication
- AES key files
- MySQL and PostgreSQL data files

After zeroizing the CSP's, the logical volumes corresponding to the following locations are also zeroized.

- /tmp
- /var/log

- /var

Also, at the end of node deletion Junos Space automatically triggers the **Zeroize** command on the node being deleted.

To zeroize your device:



CAUTION: Perform system zeroization with care. After the zeroization process is complete, no data is left on the Junos Space appliance. The Junos Space appliance and application gets into an in-accessible state other than through debug console.

1. Access the console or use SSH to view the Junos Space CLI prompt.

```
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 changes
Q> Quit
R> Redraw Menu

Choice [1-7,AQR]: 5
1> Enable Firewall
2> Disable SSH
3> Zeroize CSP

A> Apply changes
M> Return to Main Menu
R> Redraw Menu
Choice [1-3,AMR]:
```

2. To initiate the zeroization process, type **3** at the prompt:

The entire operation can take considerable time depending on the size of the media, but all critical security parameters (CSPs) are removed within a few seconds. The physical environment must remain secure until the zeroization process is complete.