JUNIPER NETWORKS | Engineering Simplicity

Security Director

Security Director Installation and Upgrade Guide

Published
2021-04-09

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.

Security Director Security Director Installation and Upgrade Guide
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 **Installing and Upgrading Security Director**

Security Director Installation Overview | 11

- Intended Audience | **12**

Setting Up a JA2500 Appliance for Security Director | 13

Setting Up a Junos Space Virtual Appliance for Security Director | 13

Upgrading Junos Space Network Management Platform | 14

Installing Security Director | 15

Upgrading Security Director | 16

Junos Space Store Overview | 19

Installing and Upgrading Security Director from the Junos Space Store | 20

2 **Setting Up and Upgrading Log Collector**

Security Director Log Collector Overview | 28

- Log Director | **29**
- Log Collector Deployment Modes | **29**
- Log Collector Storage Requirements | **29**
- Deploying Log Collector as an All-in-One Node | **30**
- Deploying Multiple Log Collectors | **31**

Deploying Log Collector as an Integrated Node | 33

Setting Up Security Director Log Collector | 34

Specifications for Deploying a Log Collector Virtual Machine | 36

Deploying Log Collector VM on a VMWare ESX Server | 37

Deploying Log Collector VM on a KVM Server | 38

Deploying Log Collector on a JA2500 Appliance | 40

Installing Integrated Log Collector on a JA2500 Appliance or Junos Space Virtual Appliance | 42

Configuring Log Collector Using Scripts | 45

Expanding the Size of the VM Disk for Log Collector | 47

JSA Log Collector Overview | 50

Adding Log Collector to Security Director | 51

Upgrading Security Director Log Collector | 53

Upgrading Log Collector VM or JA2500 Appliance | 54

Upgrading Log Collector VM or JA2500 Appliance | 56

Upgrading Log Collector CentOS Version from 6.5 to 6.8 | 58

Upgrading Integrated Log Collector | 59

Upgrading Integrated Log Collector | 59

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 install and upgrade Security Director application, set up Log Collector, add Log Collector to Security Director, and upgrade Log Collector.

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`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*

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

Convention	Description	Examples
Italic text like this	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** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• 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 *metric*>;**
| (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** **(*string1* | *string2* | *string3*)**
# (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 [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		

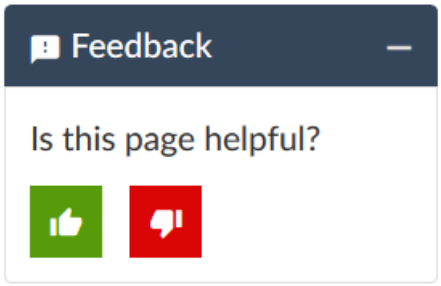
Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• 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

Installing and Upgrading Security Director

Security Director Installation Overview | **11**

Setting Up a JA2500 Appliance for Security Director | **13**

Setting Up a Junos Space Virtual Appliance for Security Director | **13**

Upgrading Junos Space Network Management Platform | **14**

Installing Security Director | **15**

Upgrading Security Director | **16**

Junos Space Store Overview | **19**

Installing and Upgrading Security Director from the Junos Space Store | **20**

Security Director Installation Overview

Security Director is a Junos Space management application designed to enable quick, consistent, and accurate creation, maintenance, and application of network security policies. It is a powerful and easy-to-use solution that lets you secure your network by creating and publishing firewall policies, IPsec VPNs, NAT policies, IPS policies, and application firewalls.

Before you install Security Director, you must configure the Junos Space Appliance as a Junos Space node.

You can install Security Director in one of the following appliances:

- Juniper Networks JA2500 Junos Space Hardware Appliance—The JA2500 appliance consists of preconfigured Junos Space Network Management Platform software. It is a dedicated hardware device that provides the computing power and specific requirements to run Security Director and the Security Director API as applications.

  The JA2500 appliance has a 2-U, rack-mountable chassis with dimensions of 17.81 in. x 17.31 in. x 3.5 in. (45.2 cm x 44 cm x 8.89 cm). The appliance has six 1-TB hard drives arranged in a RAID 10 configuration.

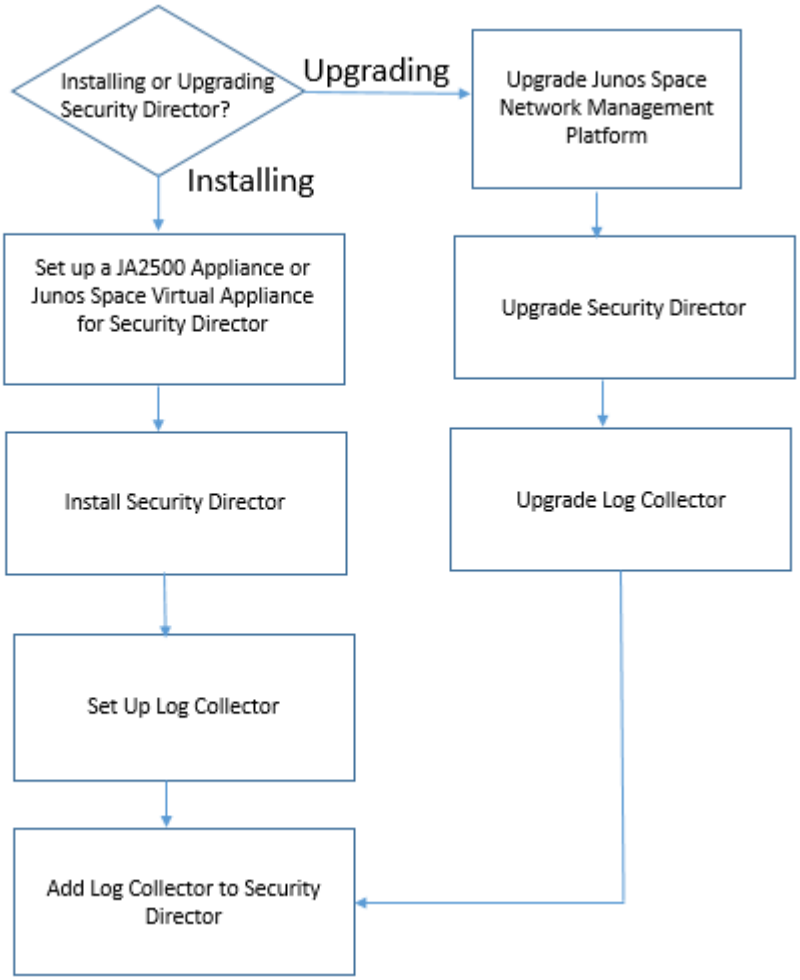
  For details about the JA2500 appliance and instructions for installation, see the Juniper Networks JA2500 Junos Space Appliance Hardware Guide.

- Junos Space Virtual Appliance—The Junos Space virtual appliance consists of preconfigured Junos Space Network Management Platform software with a built-in operating system and application stack that is easy to deploy, manage, and maintain. A Junos Space virtual appliance includes the same software and provides all the functionality available in a JA2500 appliance. You must deploy the virtual appliance on a VMware ESX server, VMware ESXi server, or a KVM server which provides a CPU, hard disk, RAM, and a network controller, but requires installation of an operating system and applications to become fully functional.

  For information about installing Junos Space virtual appliances on a VMware ESX server, VMware ESXi server, or KVM server, see the Junos Space Virtual Appliance Installation and Configuration Guide.

Figure 1 on page 12 shows the Security Director installation and upgrade flow.

Figure 1: Security Director Installation and Upgrade Flow



Intended Audience

This document is intended for network operators and administrators who install, configure, and manage the network security infrastructure.

RELATED DOCUMENTATION

Setting Up a JA2500 Appliance for Security Director | 13

Setting Up a Junos Space Virtual Appliance for Security Director | 13

Setting Up a JA2500 Appliance for Security Director

The Juniper Networks JA2500 Junos Space appliance is a dedicated hardware device that provides the computing power and specific requirements to run Security Director and the Security Director API as applications. For detailed steps on installing a JA2500 appliance, see Juniper Networks JA2500 Junos Space Appliance Hardware Guide.

You must set up the JA2500 appliance to run as a Junos Space node. To configure a JA2500 appliance as a Junos Space node, you must configure basic network and system settings to make the appliance accessible on the network. For complete configuration steps, see Configuring a Junos Space Appliance as a Junos Space Node.

RELATED DOCUMENTATION

Security Director Installation Overview | 11

Setting Up a Junos Space Virtual Appliance for Security Director

The Junos Space virtual appliance consists of preconfigured Junos Space Network Management Platform software with a built-in operating system and application stack that is easy to deploy, manage, and maintain. For more information on installing Junos Space virtual appliance, see Junos Space Virtual Appliance Installation and Configuration Guide.

You must set up the Junos Space virtual appliance to run as a Junos Space node. After you deploy a Junos Space virtual appliance, you must enter basic network and machine information to make your Junos Space virtual appliance accessible on the network. For complete configuration steps, see Configuring a Junos Space Virtual Appliance as a Junos Space Node.

RELATED DOCUMENTATION

Security Director Installation Overview | 11

Upgrading Junos Space Network Management Platform

Junos Space Security Director Release can be installed or upgraded only on the supported Junos Space Network Management Platform Release. For example, Security Director Release 21.1R1 is supported only on Junos Space Network Management Platform Release 21.1R1. If your appliance is running the supported version of Junos Space, you can skip this procedure and begin installation of Security Director. For information on supported version of Junos Space Network Management Platform for Security Director, see "Upgrading Security Director" on page 16.

If your appliance is running a Junos Space Network Management Platform release that is earlier than the supported release, you need to upgrade Junos Space Network Management Platform before upgrading Security Director.

To upgrade your Junos Space Network Management Platform:

1. Determine the installed Junos Space Network Management Platform version:
   a. Log in to Junos Space. The default username is super and password is juniper123. The Dashboard is displayed.

      Change the default credentials, when prompted.

   b. Click the **+** icon next to Administration to expand the Administration menu.

   c. Click **Applications** to list all of the applications installed.

   d. Note the version of the Junos Space Network Management Platform or the Network Application Platform. (Some earlier versions of the Network Management Platform were named Network Application Platform.) If the currently installed release is a supported one, you can skip the upgrade procedure; if not, you must upgrade the Junos Space Network Management Platform to the supported release.

2. Upgrade Junos Space Network Management Platform using the procedure at Upgrading to Junos Space Network Management Platform Release 21.1R1.

> **NOTE:** For more information about application compatibility, see the Knowledge Base article KB27572 at Junos Space Application Compatibility .

RELATED DOCUMENTATION

Setting Up a JA2500 Appliance for Security Director | 13

Setting Up a Junos Space Virtual Appliance for Security Director | 13

Installing Security Director

In Junos Space Security Director, a single image installs Security Director, Log Director, and the Security Director Logging and Reporting modules. You must deploy the Log Collector and then add it to the Security Director to view the log data in the Dashboard, Events and Logs, Reports, and Alerts pages.

NOTE: Both JSA as Log Collector and Security Director Log Collector cannot be added together.

NOTE: Upgrade to the supported release of Junos Space Network Management Platform Release. See "Upgrading Junos Space Network Management Platform" on page 14.

To install the Junos Space Security Director:

1. Download the Junos Space Security Director Release image from the download site.

2. Install the Security Director application using the procedure at Adding a Junos Space Application.

RELATED DOCUMENTATION

Upgrading Junos Space Network Management Platform | 14

Upgrading Security Director | 16

Setting Up Security Director Log Collector | 34

Junos Space Store Overview | 19

Installing and Upgrading Security Director from the Junos Space Store | 20

Upgrading Security Director

You can upgrade from a previous Security Director release to the latest Security Director release.

Before You Begin

- If you are upgrading from a previous version of Security Director, clear your browser cache before accessing the Security Director user interface.
- Back up Junos Space Security Director Release that you want to upgrade. You must take the backup before upgrading Junos Space Network Management Platform. Backing up the Junos Space Network Management Platform database before the upgrade helps you to recover the data if the upgrade fails. See Backing Up the Junos Space Network Management Platform Database.
- You must upgrade to the supported Junos Space Network Management Platform Release, before you upgrade the Security Director, Log Director, and Security Director Logging and Reporting modules. See "Upgrading Junos Space Network Management Platform" on page 14.
- The Junos Space Network Management Platform should be active and functioning.

> **NOTE:** The Required Platform Version column in Table 3 on page 16 indicates the supported Junos Space Network Management Platform version. Before upgrading Security Director, ensure that the system is running the supported Junos Space Network Management Platform version. See "Upgrading Junos Space Network Management Platform" on page 14.

Table 3: Upgrade Path

Upgrading to Release	Required Platform Version	Upgrade Path	Description
Security Director 21.1R1	21.1R1	• 20.3R1 > 21.1R1	You can upgrade from the following releases: • Junos Space Network Management Platform Release 20.3R1 and Security Director Release 20.3R1

Table 3: Upgrade Path *(continued)*

Upgrading to Release	Required Platform Version	Upgrade Path	Description
Security Director 20.3R1	20.3R1	• 19.3R1 > 20.3R1 • 19.4R1 > 20.3R1 • 20.1R1 > 20.3R1	You can upgrade from the following releases: • Junos Space Network Management Platform Release 19.3R1 and Security Director Release 19.3R1 • Junos Space Network Management Platform Release 19.4R1 and Security Director Release 19.4R1 • Junos Space Network Management Platform Release 20.1R1 and Security Director Release 20.1R1
Security Director 20.1R1	20.1R1	• 19.3R1 > 20.1R1 • 19.4R1 > 20.1R1	You can upgrade from the following releases: • Junos Space Network Management Platform Release 19.3R1 and Security Director Release 19.3R1 • Junos Space Network Management Platform Release 19.4R1 and Security Director Release 19.4R1
		You can now perform direct upgrade to 20.1R1 from earlier versions of Junos Space Security Director Release 19.1R1 and 19.2R1. • 19.1R1 > 20.1R1 • 19.2R1 > 20.1R1 **NOTE:** You can perform direct upgrade only for Junos Space Security Director. However, you must follow all the supported upgrade paths for Junos Space Network Management Platform and Log Collector to upgrade to 20.1R1.	
Security Director 19.4R1	19.4R1	• 19.2R1 > 19.4R1 • 19.3R1 > 19.4R1	You can upgrade from the following releases: • Junos Space Network Management Platform Release 19.2R1 and Security Director Release 19.2R1 • Junos Space Network Management Platform Release 19.3R1 and Security Director Release 19.3R1
Security Director 19.3R1	19.3R1	• 19.2R1 > 19.3R1 • 19.1R2 > 19.3R1 • 19.1R1 > 19.3R1	You can upgrade from the following releases: • Junos Space Network Management Platform Release 19.2R1 and Security Director Release 19.2R1 • Junos Space Network Management Platform Release 19.1R1 and Security Director Release 19.1R2 • Junos Space Network Management Platform Release 19.1R1 and Security Director Release 19.1R1

Table 3: Upgrade Path *(continued)*

Upgrading to Release	Required Platform Version	Upgrade Path	Description
Security Director 19.2R1	19.2R1	• 19.1R2 > 19.2R1 • 19.1R1 > 19.2R1 • 18.4R1 > 19.2R1	You can upgrade from the following releases: • Junos Space Network Management Platform Release 19.1R1 and Security Director Release 19.1R2 • Junos Space Network Management Platform Release 19.1R1 and Security Director Release 19.1R1 • Junos Space Network Management Platform Release 18.4R1 and Security Director Release 18.4R1
Security Director 19.1R2	19.1R1	• 19.1R1 > 19.1R2 • 18.4R1 > 19.1R2 • 18.3R1 > 19.1R2	You can upgrade from the following releases: • Junos Space Network Management Platform Release 19.1R1 and Security Director Release 19.1R1 • Junos Space Network Management Platform Release 18.4R1 and Security Director Release 18.4R1 • Junos Space Network Management Platform Release 18.3R1 and Security Director Release 18.3R1
Security Director 19.1R1	19.1R1	• 18.4R1 > 19.1R1 • 18.3R1 > 19.1R1	You can upgrade from the following releases: • Junos Space Network Management Platform Release 18.4R1 and Security Director Release 18.4R1 • Junos Space Network Management Platform Release 18.3R1 and Security Director Release 18.3R1
		You can now perform direct upgrade to 19.1R1 from earlier versions of Junos Space Security Director Release 18.2R1, 18.1R1, and 17.2R2. • 18.2R1 > 19.1R1 • 18.1R1 > 19.1R1 • 17.2R2 > 19.1R1 **NOTE:** You can perform direct upgrade only for Junos Space Security Director. However, you must follow all the supported upgrade paths for Junos Space Network Management Platform to upgrade to 19.1R1.	

To upgrade from a previous version of Junos Space Security Director:

1. Download the Junos Space Security Director Release image to which you want to upgrade from the download site.

2. Upgrade the Junos Space Security Director application using the procedure at Upgrading a Junos Space Application.

> **NOTE:**
> - If you try to upload Junos Space Security Director image of a lower version, an error message **Can only upgrade to newer version** appears. Click **OK** and upload compatible version of Junos Space Security Director.
> - If you try to upload incompatible version of Junos Space Security Director image, an error message **Current platform version does not support this software version** appears . Click **OK** and upload compatible version of Junos Space Security Director.

RELATED DOCUMENTATION

Upgrading Junos Space Network Management Platform | 14

Installing Security Director | 15

Junos Space Store Overview | 19

Installing and Upgrading Security Director from the Junos Space Store | 20

Junos Space Store Overview

The Junos Space store displays the latest compatible versions of the Junos Space applications, which can be installed or upgraded on the current version of Junos Space Network Management Platform. Starting in Junos Space Security Director Release 18.2R1, you can install or upgrade Junos space Security Director application from the Junos Space store on the Network Management Platform.

You must configure the Juniper Networks Software download credentials to connect to Junos Space store. The Junos Space store lists the latest available applications.

The Junos Space Network Management Platform accesses the metadata repository hosted by Juniper Networks to discover the available applications and published versions. When the user initiates an install or upgrade for Security Director application or its components, the package path is identified from the metadata file and package is downloaded. This reduces the manual effort of downloading the application package from the download site and then uploading it to the Junos Space Network Management Platform server, thereby enhancing the installation and upgrade process.

You can view whether a Security Director application version is supported on the current Junos Space Network Management Platform version, even before initiating install or upgrade. Junos Space store allows

the component configuration while installing Security Director. It limits the component configuration when user tries to upgrade Security Director. Therefore, refer the existing method of upgrading Log Collector and Policy Enforcer components after upgrading the Security Director application.

> **NOTE:** The earlier method of installing and Upgrading Security Director application documented in "Installing Security Director" on page 15 and "Upgrading Security Director" on page 16 are still applicable. You can choose to install using the existing method or through the Junos Space store.

RELATED DOCUMENTATION

Installing and Upgrading Security Director from the Junos Space Store | 20

Installing and Upgrading Security Director from the Junos Space Store

The Junos Space store displays a list of applications, which can be installed on the Junos Space Network Management Platform. This topic describes the Security Director installation and upgrade procedure using the Junos Space store.

Before You Begin

- Configure Junos Space Store in Junos Space Network Management Platform. For details on configuring and modifying the Junos Space settings, see Configuring and Managing Junos Space Store.
- You must deploy the Log Collector and Policy Enforcer nodes before installing Security Director.
- Ensure the HDD size (>500GB) of the Junos Space Platform before configuring Log Collector. OpenNMS should be in the disabled state.

For configuring Log Collector component in Junos Space store:

- For distributed deployment of Security Director Log Collector, deploy Log Collector VM on a VMWare ESX server, KVM server, or a JA2500 appliance. To know more about distributed deployment, see "Setting Up Security Director Log Collector" on page 34.

- For integrated deployment of Log Collector, install the Integrated Log Collector on a JA2500 Appliance or Junos Space virtual appliance. To know more about the integrated deployment of Log Collector, see, "Setting Up Security Director Log Collector" on page 34.
- Deploy and configure JSA for using JSA as Log Collector. See, "JSA Log Collector Overview" on page 50.

For configuring Policy Enforcer component in Junos Space Store:

- Deploy and configure Policy Enforcer. See, *Installing Policy Enforcer* in Administration Guide.

To install and upgrade Security Director from the Junos Space Store:

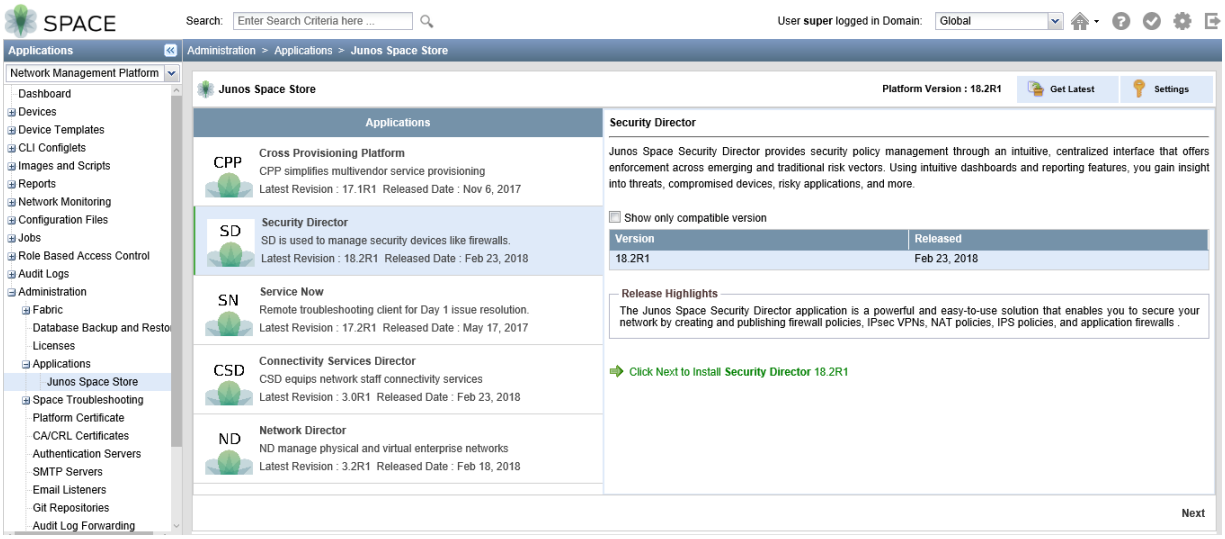
1. Log in to Junos Space Network Management Platform.
2. Select **Administration** > **Applications** > **Junos Space Store**.

   The Junos Space Store page appears.

   > **NOTE:** Click **Get Latest** to refresh the list of applications in Junos Space store.

   The Junos Space store with all the applications are displayed as shown in Figure 2 on page 21.

Figure 2: Junos Space Store



3. Select **Security Director**.

   The details of the application such as the compatible versions, version release date, and release highlights are displayed.

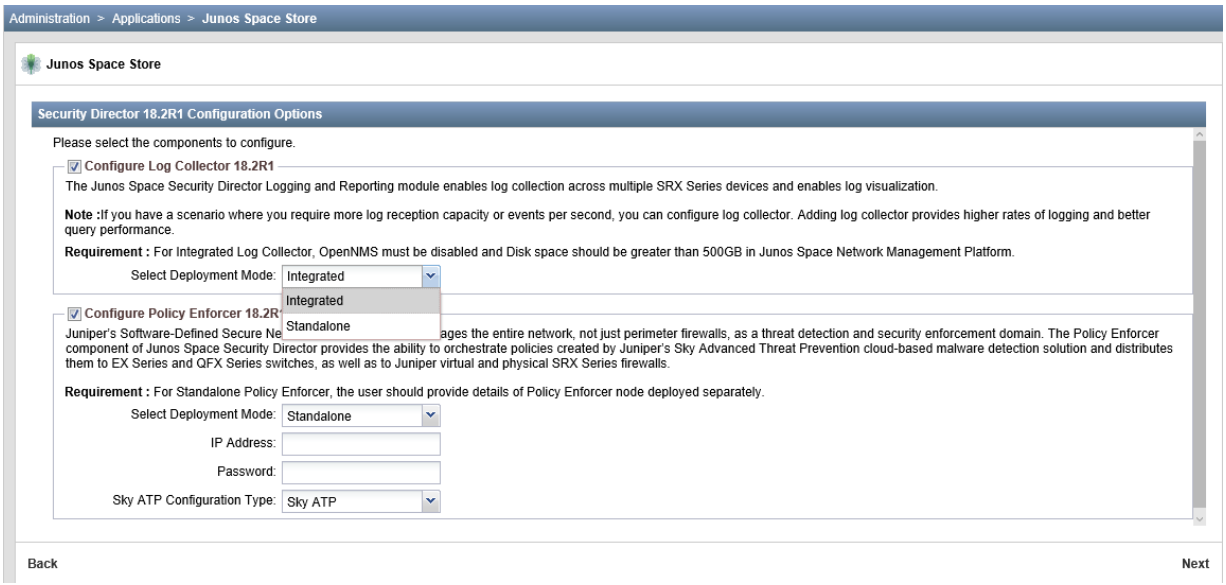
> **NOTE:** Click **Show only compatible version** option to display only the Security Director versions supported on the current platform version.

4. Select a version to be installed or upgraded and click **Next**

> **NOTE:** If the selected version is not compatible with the Junos Space Network Management Platform version, a warning message is displayed.

The Security Director configuration options are displayed as shown in Figure 3 on page 22.

Figure 3: Security Director Components



5. Select the components, which you want to configure and complete the configuration according to the guidelines given in Table 4 on page 24.

> **NOTE:** User can configure Log Collector and Policy Enforcer if already deployed and available. The previous method of adding the Log Collector and Policy Enforcer from Security Director is also applicable.

NOTE: Junos Space store allows the component configuration while installing Security Director. Upgrade of components like Log Collector and Policy Enforcer is not handled by Junos Space Store. Therefore, refer the existing method of upgrading Log Collector and Policy Enforcer components after upgrading the Security Director application.

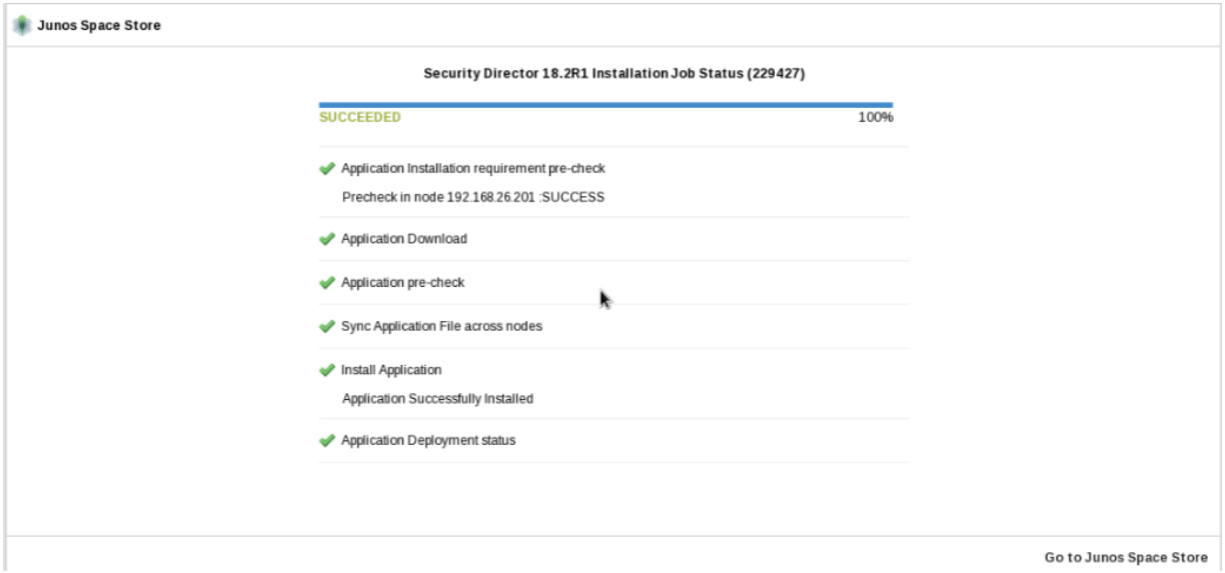
6. Click **Next**.

   The Security Director terms and conditions and the license agreement is displayed. Review the license agreement.

7. Click **Accept and Install**.

   The job status is displayed as shown in Figure 4 on page 23.

Figure 4: Job Status



8. Click **Go to Junos Space Store**.

   The installed or upgraded version of Security Director is displayed in the Junos Space store as shown in Figure 5 on page 24.

Figure 5: Verifying the Installed or Upgraded Version

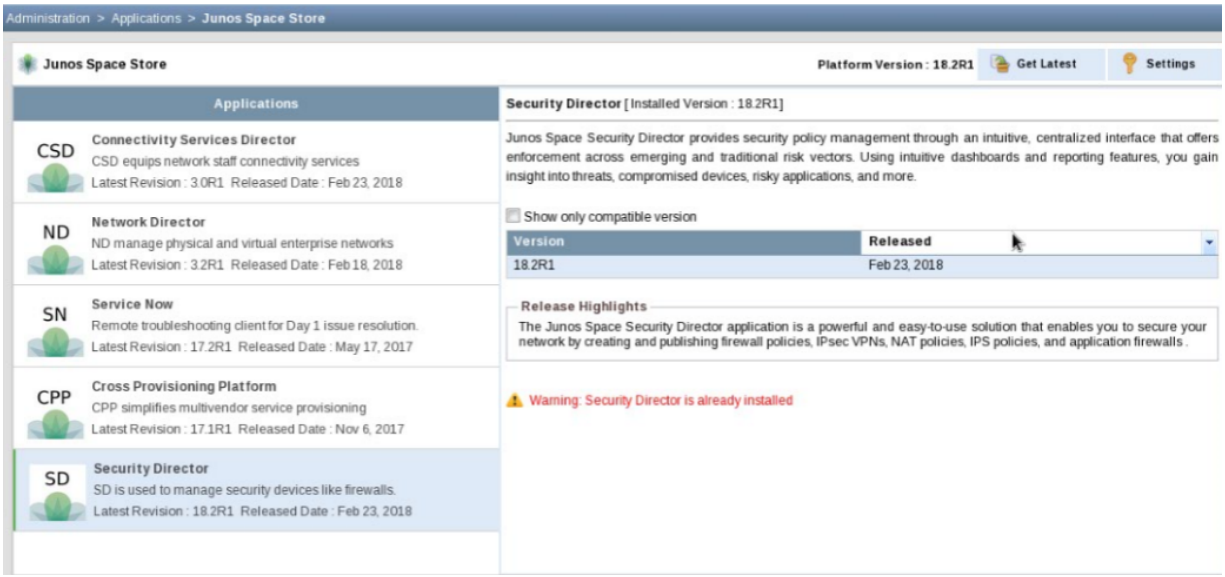


Table 4: Security Director Components Description

Fields	Description
Log Collector	
Deployment Mode	Select one of the following: • Integrated—The integrated Log Collector is installed on Junos Space node (JA2500 appliance or virtual appliance). Integrated Log Collector on a JA2500 appliance or Junos Space virtual appliance supports only 500 eps. **NOTE:** For Integrated Log Collector, OpenNMS must be disabled. On the Junos Space Network Management Platform, the disk space must be greater than 500GB. • Standalone—Standalone log collector VM is deployed separately on a VMWare ESX Server, KVM Server, or JA2500 appliance. **NOTE:** The fields Node Type, Node Name, IP Address, and Username and Password are applicable only if the deployment mode is Standalone.
Node Type	Select one of the following: • Security Director Log Collector • Juniper Secure Analytics **NOTE:** You can add only Log Receiver node in Security Director and cannot add Log Storage node.

Table 4: Security Director Components Description *(continued)*

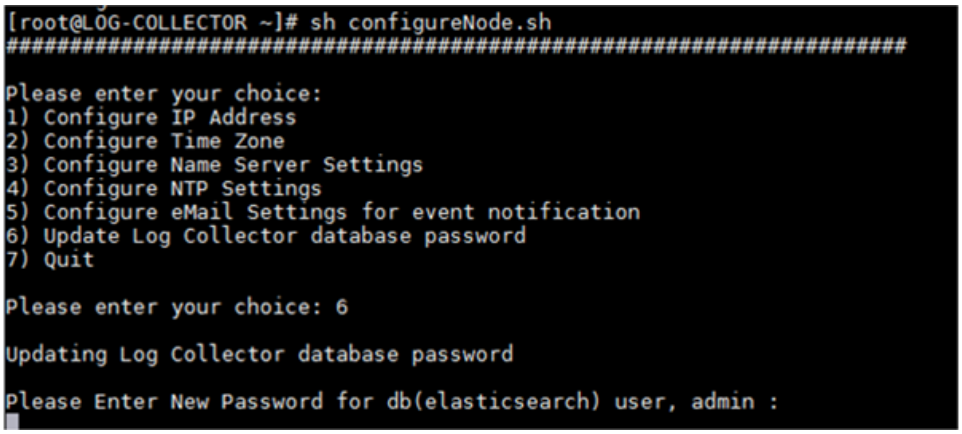
Fields	Description
Node Name	Enter the Node name.
IP Address	Enter the IPv4 or IPv6 address.
Username and Password	For Security Director Log Collector, provide the default credentials; username is admin and password is juniper123. Change the default password using the Log Collector CLI **configureNode.sh** command as shown in Figure 6 on page 25. **Figure 6: Change Password**  For JSA, provide the admin credentials that is used to login to the JSA console.
Policy Enforcer	
Deployment Mode	Select Standalone. **NOTE:** For Policy Enforcer, only Standalone option is available.
IP Address	Specify the IP address of the Policy Enforcer virtual machine.
Password	Enter the password to login to the virtual machine with the root credentials.

Table 4: Security Director Components Description *(continued)*

Fields	Description
Sky ATP Configuration Type	Select one of the following configuration types: • Sky ATP—Includes all threat prevention types, but does not include the benefits of Secure Fabric, Policy Enforcement Groups, and Threat Prevention policies provided by Policy Enforcer. All enforcement is done through SRX Series Device policies. • Cloud Feeds Only—The prevention types available are command and control server, infections hosts, and Geo IP feeds. Policy Enforcer Secure Fabric, Policy Enforcement Groups, and Threat Prevention policies are also available. All enforcement is done through SRX Series Device policies. • Sky ATP with SDSN—A full version of the product. All Policy Enforcer features and threat prevention types are available. • None—There are no feeds available from Sky ATP, but the benefits of Secure Fabric, Policy Enforcement Groups, and Threat Prevention policies provided by Policy Enforcer are available. Infected hosts is the only prevention type available.
Network End Point	Polling timers affect how often the system polls to discover endpoints. The timer polls infected endpoints moving within the sites that are a part of Secure fabric. You can set this range from 2 minutes to 60 minutes. The default is 5 minutes.
PollSite End Point	Polling timers affect how often the system polls to discover endpoints. The timer polls all endpoints added to the secure fabric. You can set this range between 1 to 48 hours. The default is 24 hours.

RELATED DOCUMENTATION

Junos Space Store Overview | 19

2

CHAPTER

Setting Up and Upgrading Log Collector

Security Director Log Collector Overview | 28

Setting Up Security Director Log Collector | 34

JSA Log Collector Overview | 50

Adding Log Collector to Security Director | 51

Upgrading Security Director Log Collector | 53

Security Director Log Collector Overview

IN THIS SECTION

- Log Director | 29
- Log Collector Deployment Modes | 29
- Log Collector Storage Requirements | 29
- Deploying Log Collector as an All-in-One Node | 30
- Deploying Multiple Log Collectors | 31
- Deploying Log Collector as an Integrated Node | 33

The Junos Space Security Director Logging and Reporting module enables log collection across multiple SRX Series devices and enables log visualization.

You can set up Log Collector on a VM or a JA2500 appliance. You can configure Log Collector as an All-in-One node or integrated node for small-scale deployments. For larger deployments, begin with a single Log Receiver node and Log Storage node, and incrementally add Log Storage nodes as your needs expand. You can have a maximum of one Log Receiver node and three Log Storage nodes.

You need to set up the Log Collector VM and deploy the Log Collector as an All-in-One node, Log Storage Node, or Log Receiver Node.

The following node types are supported:

- All-in-One node
- Log Receiver node
- Log Storage node
- Integrated node

NOTE:

- You can configure eth0 or eth1 for receiving logs from devices in different Log Collector deployment modes.
- High Availability is not supported on Security Director Log Collector. However, JSA as Log Collector supports High Availability.
- Security Director Logging and Reporting is not supported on JA1500 appliance.

Log Director

Log Director is an application on Junos Space Network Management Platform that gets installed as part of Security Director installation. It is used for system log data collection for SRX and vSRX Series devices running Junos OS. Log Director consists of two components:

- Junos Space application
- VM or JA2500 deployment of Log Collector node(s)

Log Collector Deployment Modes

Table 5 on page 29 describe different modes in which Log Collector can be deployed.

Table 5: Log Collector Deployment Modes

Node Type	Description
All-in-One Node (Combined deployment)	Both the Log Receiver and Log Storage nodes run on the same VM or JA2500 appliance. It supports up to 3,000 eps with spinning disks and 4,000 eps with SSD drives. All-in-One node is suitable for demos and small-scale deployments.
Log Receiver Node (Distributed deployment)	The Log Receiver node receives system logs from SRX Series devices and vSRX Series devices and forwards them to a Log Storage node. You can configure up to three Log Storage nodes. You must configure the IP address of the Log Receiver Node on SRX and vSRX Series devices and the IP address of the Log Storage nodes on the Log Receiver node.
Log Storage Node (Distributed deployment)	This node analyzes, indexes, and stores the system logs. It receives the system logs from Log Receiver node.
Integrated	It is similar to an All-in-One node. It is installed on a Junos Space node (JA2500 appliance or virtual appliance) and it works as both the Log Receiver node and Log Storage node.

Log Collector Storage Requirements

The total storage required for retaining X number of days at a given events per second (eps) rate is:

eps * 0.155 * X = Total storage (in GB)

For example, the storage requirement for 7 days at 500 eps is 500 * 0.155 * 7 = 542 GB, with a +20% margin. The storage space is allocated and equally distributed to the Log Storage nodes.

NOTE: The logs get rolled over under the following scenarios:

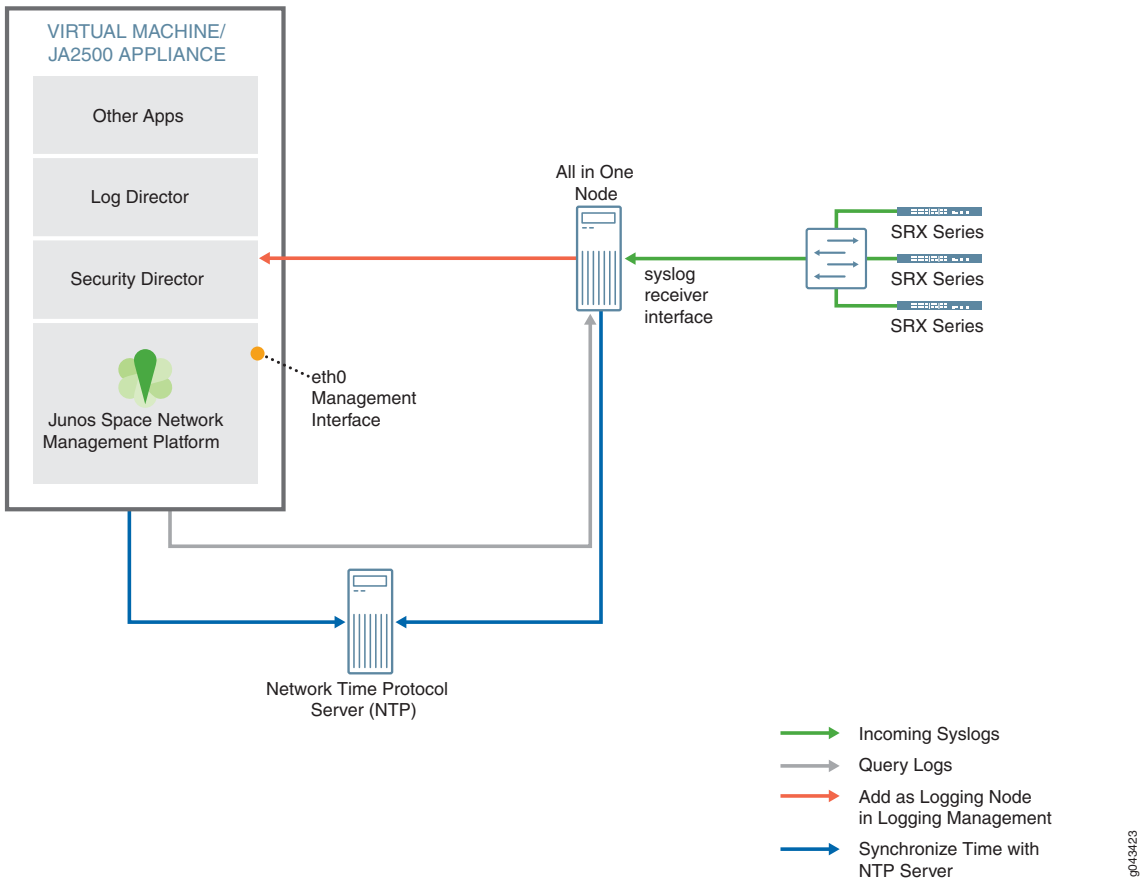
- Time-based rollover—Logs that are older than 45 days are automatically rolled over, even if the disk space is available.
- Disk size-based rollover—Older logs get rolled over when the disk size reaches 400 GB.

Deploying Log Collector as an All-in-One Node

An All-in-One node acts both as the Log Receiver and Log Storage node. For a VM environment, a single OVA image is used to deploy the All-in-One, Log Receiver, and Log Storage nodes. The image presents a configuration script after you log in and you must select All-in-One to configure the node. For JA2500 deployments, a single ISO image is used to install the All-in-One, Log Receiver, and Log Storage nodes. During setup, you can configure the node as an All-in-One node.

Figure 7 on page 31 shows an example of an All-in-One node deployment.

Figure 7: All-in-One Node Deployment



Deploying Multiple Log Collectors

If you have a scenario where you require more log reception capacity or events per second, you can add multiple logging nodes. Multiple logging nodes provide higher rates of logging and better query performance. You can add a maximum of one Log Receiver node and three Log Storage nodes.

For a VM environment, a single OVA image is used to deploy a Log Receiver node and a Log Storage node. The image presents a configuration script after you log in. During setup, you can configure the node as either a Log Receiver or Log Storage node. At deployment, the user must select the memory and CPU configuration values, as appropriate for the VM or JA2500 appliance.

For JA2500 deployments, a single ISO image is used to install the Log Receiver and Log Storage nodes. During setup, you can configure the node as either a Log Receiver or a Log Storage node.

Figure 8 on page 32 shows the deployment example using multiple nodes for up to 10K eps.

Figure 8: Using Multiple Nodes for Up to 10K eps

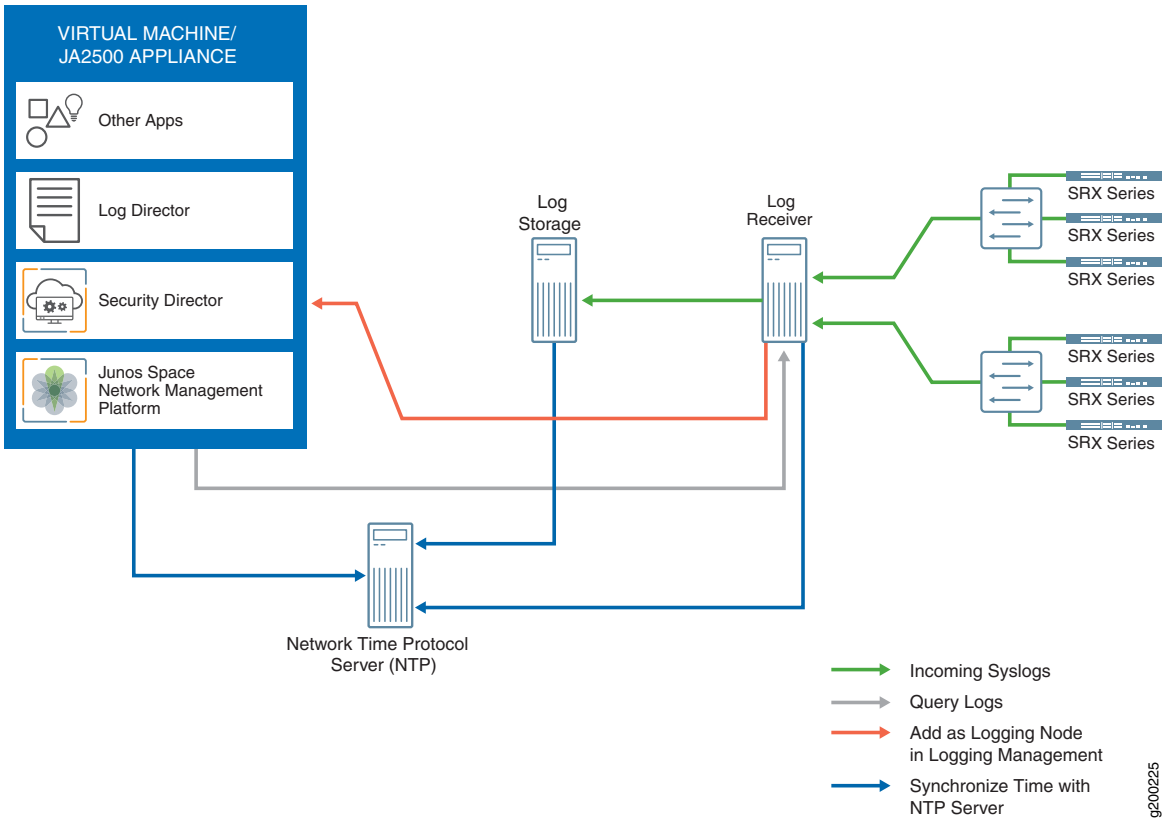
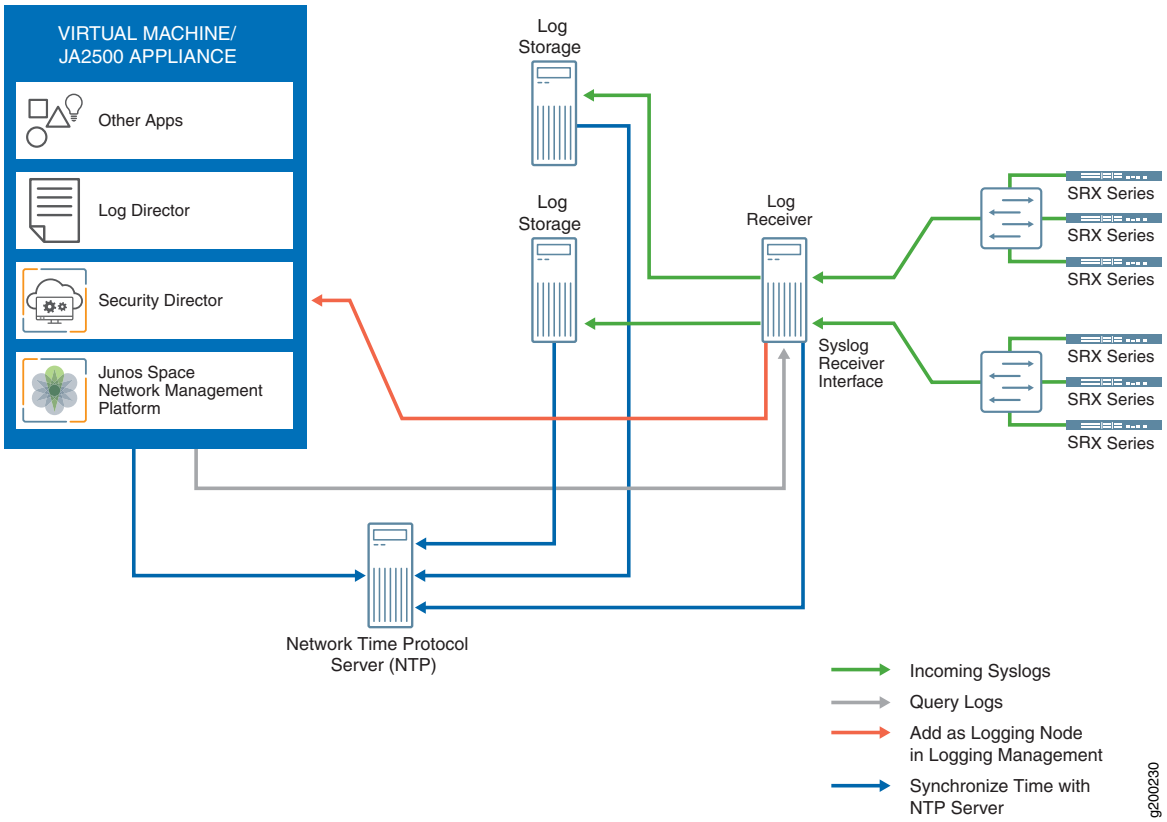


Figure 9 on page 33 shows the deployment example using multiple nodes for greater than 10K eps.

Figure 9: Using Multiple Nodes for Greater Than 10K eps

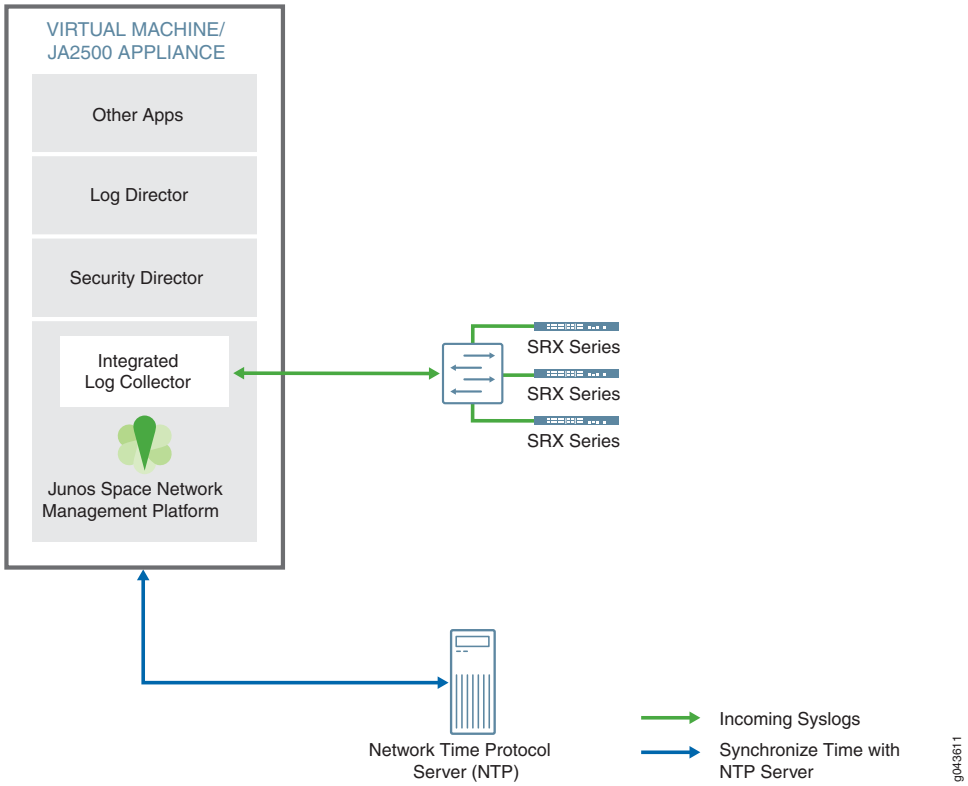


Deploying Log Collector as an Integrated Node

It is installed on a Space node (JA2500 appliance or virtual appliance) and it works as both the Log Receiver node and Log Storage node. You must use the Integrated Log Collector installer for Space application package to install integrated Log Collector on JA2500 appliance or virtual appliance.

NOTE: Integrated Log Collector is not a feasible solution in Junos Space high-availability (HA) mode. We recommended you to use All-in-one virtual machine or JSA as a Log Collector for Junos Space HA mode.

Figure 10: Integrated Node Deployment



RELATED DOCUMENTATION

- Upgrading Junos Space Network Management Platform | 14
- Installing Security Director | 15
- Upgrading Security Director | 16
- Setting Up Security Director Log Collector | 34

Setting Up Security Director Log Collector

IN THIS SECTION

- Specifications for Deploying a Log Collector Virtual Machine | 36
- Deploying Log Collector VM on a VMWare ESX Server | 37

- Deploying Log Collector VM on a KVM Server | 38
- Deploying Log Collector on a JA2500 Appliance | 40
- Installing Integrated Log Collector on a JA2500 Appliance or Junos Space Virtual Appliance | 42
- Configuring Log Collector Using Scripts | 45
- Expanding the Size of the VM Disk for Log Collector | 47

NOTE: You must use 20.1R1 Log Collector builds for Security Director Release 21.1R1. There are no Log Collector builds for 21.1R1 release. When you upgrade Security Director release to 21.1R1, you must use Log Collector 20.1R1.

The prerequisites for setting up Log Collector are as follows:

- Make sure that the JA2500 appliance or VM is running supported release of Junos Space Network Management Platform and Junos Space Security Director.
- The Junos Space Network Management Platform must be active and functioning.
- The following ports are required for Log Collector to function and these ports must be open between the Junos Space server and the Log Collector:
  - Port 8004 (TCP)—For communication between the Junos Space server and the Log Collector node agent
  - Port 8003 (TCP)—For log data queries
  - Port 9200 (TCP)—For Log Storage nodes
  - Port 9300 (TCP)—For communicating across elasticsearch cluster
  - Port 4567 (TCP)—For communication between the Log Receiver node and Log Storage node
  - Port 514 (TCP)—For receiving system logs
  - Port 514 (UDP)—For receiving system logs
  - Port 22 (TCP)—For SSH connectivity
  - Port 4514 (TCP)—Used for TCP forwarding
- The following ports are not required for Log Collector to function, but they are used by other peripheral services:
  - Port 5671 (TCP)
  - Port 32803 (TCP)

- Port 32769 (UDP)

See the following topics for information about deploying Log Collector:

Specifications for Deploying a Log Collector Virtual Machine

You can use the tables below to decide if you require a single Log Collector or multiple Log Collectors.

The following tables describe the VM configuration with Solid State Drives (SSD) and with non Solid State Drives. They list the required specifications for deploying a Log Collector VM for various events per second (eps) rates. The eps rates shown in the tables were achieved in a testing environment. Your results might differ, depending on your configuration and network environment.

Table 6: With Solid State Drives (SSD)

	Log Receiver Node			Log Storage Node			
Setup	Number of Nodes	CPU	Memory	Number of Nodes	CPU	Memory	Total Nodes
4K eps	1	4	16 GB	-	-	-	1
10K eps	1	8	32 GB	1	8	64 GB	2
20K eps	1	8	32 GB	2	8	64 GB	3

Table 7: With Non-Solid State Drives

	Log Receiver Node			Log Storage Node			
Setup	Number of Nodes	CPU	Memory	Number of Nodes	CPU	Memory	Total Nodes
3K eps	1	4	16 GB	-	-	-	1
10K eps	1	8	32 GB	2	8	64 GB	3
20K eps	1	8	32 GB	3	8	64 GB	4

NOTE: VMs with 64 GB memory provide better stability for log storage.

Deploying Log Collector VM on a VMWare ESX Server

> **NOTE:** Install VMware vSphere or vCenter client on your local system.

To deploy Log Collector VM on a VMware ESX server:

1. Download the latest Log Collector open virtual appliance (OVA) image from the download site.
2. Using VMware vSphere or vCenter client, deploy the Log Collector OVA image onto the VMware ESX server.
3. Edit the CPU and memory as per the system requirement for the required events per second (eps) as shown in Table 6 on page 36 and Table 7 on page 36.
4. Power on the Log Collector VM.
5. Use the default credentials to log in to Log Collector. The username is **root** and password is **juniper123**.
6. Change the default password of the VM.
7. Select one of the following node types:
   - Enter **1** to deploy Log Collector as an All-in-One node.
   - Enter **2** to deploy Log Collector as a Log Receiver node.
   - Enter **3** to deploy Log Collector as a Log Storage node.
8. Configure your network settings.

After setting up the Log Collector, add the Log Collector node to Security Director. See “Adding Log Collector to Security Director” on page 51.

> **NOTE:** Using VMware vSphere Client version 5.5 and earlier, you cannot edit the settings of virtual machines of version 10 or later. See VMware Knowledge Base.

Deploying Log Collector VM on a KVM Server

You can deploy Log Collector VM on a kernel-based virtual machine (KVM) server installed on CentOS Release 6.8.

Before You Begin

- The KVM server and supported packages must be installed on a machine running CentOS Release 6.8 with the required kernels and packages. See http://wiki.centos.org/HowTos/KVM.
- Install the Virtual Machine Manager (VMM) client on your local system.
- Configure the bridge interface according to your environment. You must have at least two static IP addresses that are unused.

> **NOTE:** We recommend you to install the Log Collector virtual machine on a KVM server using VMM.

To deploy Log Collector VM on a KVM server:

1. Download the Log Collector KVM image from the download site on the KVM host and extract the tgz file, which contains the **system.qcow2** and **data.qcow2** files.

2. Launch the VMM client by typing **virt-manager** from your terminal or from the Applications menu, click **System Tools** and select Virtual Machine Manager.

   The Virtual Machine Manager window appears.

3. Select **File** > **New Virtual Machine** to install a new virtual machine.

   The new VM dialog box appears.

4. In the new VM dialog box:

   a. Select **Import existing disk image** and click **Next**.

   b. Click **Browse** and then select the **system.qcow2** file.

   c. Select **Linux** as the operating system and the version as **Red Hat Enterprise Linux 6.6 or later**.

d. Click **Forward**.

e. Set the CPU settings as **4** , and then select or enter the minimum memory (RAM) value as **16384** MB.

5. Click **Forward**.

6. Edit the **Name** field, select or set up the network for each bridge or interface configured, and select the **Customize Configuration Before Install** option.

7. Click **Finish**.

8. Select the Storage option from the left navigation on the Add New Virtual Hardware window, and then click **Add Hardware**.

9. On the Storage window:

   a. Click **Select managed or other existing storage** and choose the **data.qcow2** file.

   b. Select the storage format as **qcow2** under Advanced Options.

   c. Click **Finish**.

10. Select one of the following node types:

    - Enter 1 to deploy Log Collector as an All-in-One node.
    - Enter 2 to deploy Log Collector as a Log Receiver node.
    - Enter 3 to deploy Log Collector as a Log Storage node.

11. Click **Begin Installation** to start the Log Collector VM.

12. After the installation, you can configure the IP address, name server, and time zone.

After setting up the Log Collector, add the Log Collector node to Security Director. See “Adding Log Collector to Security Director” on page 51.

Deploying Log Collector on a JA2500 Appliance

You can deploy Log Collector on a JA2500 appliance. To install the Log Collector on the JA2500 appliance using a USB flash drive, you must create a bootable USB flash drive, install the Log Collector node using the USB flash drive, and add the Log Collector node to Security Director.

> **NOTE:** Before creating a bootable USB flash drive, download and install Rufus software on your system.

To create a bootable USB flash drive:

1. Plug the USB flash drive into the USB port of a laptop or PC.
2. Download the Log Collector ISO image from the download site to your laptop or PC.

If you are using a computer with Microsoft Windows as the operating system, follow these steps to create a bootable USB flash drive:

1. Open Rufus software installed on your computer.

   The Rufus window opens.
2. Select the USB storage device from the Device list.
3. Select the ISO image downloaded in Step 2 in the Format options section. Click the open or browse icon next to the Create a bootable disk using option to select the ISO image.
4. Click **Start**.

   A progress bar indicates the status of the bootable USB flash drive creation. A success message is displayed once the process completes successfully.
5. Click **Exit** to exit the window.
6. Eject the USB flash drive and unplug it from the computer.

To install Log Collector using a USB flash drive:

1. Power down the JA2500 appliance.
2. Plug the USB flash drive into the USB port of the JA2500 appliance.

3. Perform the following steps to access the JA2500 appliance boot menu:
   a. Power on the JA2500 appliance.
   b. While the JA2500 appliance powers on, press the key mapped to send the DEL character in the terminal emulation utility.

      NOTE: Typically, the Backspace key is mapped to send the DEL character.

   c. The boot menu appears after a few minutes.
4. Ensure that the USB boot is at the top of the appliance boot-priority order.

   If USB KEY: CBM USB 2.0 - (USB 2.0) is not at the top of the list, perform the following steps:
   a. Use the Down Arrow key to select USB KEY:CBM USB 2.0- (USB 2.0), and use the + key to move the entry to the top of the list.
   b. Press the F4 key to save your changes and exit the BIOS setup.
5. After Verifying the BIOS setting, power off the JA2500 appliance.
6. Power on the appliance again. The boot menu displays the following options:
   a. Install Log Collector on Juniper JA2500 Hardware.
   b. Boot from local drive.
7. Select **Install Log Collector on Juniper JA2500 Hardware**.
8. Power off the appliance once the installation is completed.
9. Restart the appliance and select **Boot from local drive**.
10. Use the default credentials to log in to the JA2500 appliance; username is **root** and password is **juniper123**.
11. Change the default password.
12. After logging in, select the desired Log Collector node type.
    - Enter 1 to deploy Log Collector as an All-in-One node.

- Enter 2 to deploy Log Collector as a Log Receiver node.
- Enter 3 to deploy Log Collector as a Log Storage node.

13. Configure the IP address and gateway.

14. Configure settings for the DNS name server and the NTP server.

After setting up the Log Collector, add the Log Collector node to Security Director. See "Adding Log Collector to Security Director" on page 51.

Installing Integrated Log Collector on a JA2500 Appliance or Junos Space Virtual Appliance

You can install an integrated Log Collector on a JA2500 appliance or Junos Space virtual appliance. The integrated Log Collector is installed on Junos Space node (JA2500 appliance or virtual appliance) and it works as both the Log Receiver node and Log Storage node. Integrated Log Collector supports only 500 eps.

Before You Begin

- Integrated Log Collector uses the 9200, 514, and 4567 ports.
- Junos Space Network Management Platform must be configured with Ethernet Interface eth0 and management IP addresses.
- OpenNMS must be disabled on Junos Space Network Management Platform.
- Ethernet Interface eth0 on the Junos Space Network Management Platform must be connected to the network to receive logs.
- /var should have a minimum of 500-GB disk space for the integrated Log Collector installation to complete.

Table 8 on page 42 shows the specifications for installing the integrated Log Collector on a JA2500 appliance.

Table 8: Specifications for Installing an Integrated Log Collector on a JA2500 appliance

Component	Specification
Memory	8 GB Log Collector uses 8 GB of the available 32-GB system RAM.

Table 8: Specifications for Installing an Integrated Log Collector on a JA2500 appliance *(continued)*

Component	Specification
Disk space	500 GB This is used from the existing JA2500 appliance disk space.
CPU	Single core

NOTE: These specifications are used internally by the integrated Log Collector on JA2500 appliance.

Table 9 on page 43 shows the specifications for installing the integrated Log Collector on Junos Space virtual appliance.

Table 9: Specifications for Installing an Integrated Log Collector on a Junos Space Virtual Appliance

Component	Specification
Memory	8 GB If integrated Log Collector is running on the Junos Space virtual appliance, we recommend that you add 8 GB of RAM to maintain the Junos Space performance. It uses 8 GB of system RAM from the total system RAM.
Disk space	500 GB Minimum 500 GB free space is required. You can add any amount of disk space.
CPU	2 CPUs of 3.20 GHz

NOTE: These specifications are used internally by the integrated Log Collector running on the Junos Space virtual appliance.

To install an integrated Log Collector on a JA2500 appliance or virtual appliance:

1. Download the integrated Log Collector script from the download site.
2. Copy the integrated Log Collector script to a JA2500 appliance or virtual appliance.
3. Connect to the CLI of JA2500 appliance or virtual appliance with admin privileges.

4. Navigate to the location where you have copied the integrated Log Collector script.

5. Change the file permission using the following command:

   chmod +x Integrated-Log-Collector-xx.xxx.xxx.sh

   For example, **chmod +x Integrated-Log-Collector-20.1R1.xxx.sh**

6. Install the integrated Log Collector script using the following command:

   ./Integrated-Log-Collector-xx.xxx.xxx.sh

   For example, **./Integrated-Log-Collector-20.1R1.xxx.sh**

   - The installation stops if the following error message is displayed while installing the integrated Log Collector on the virtual appliance. You must expand the virtual appliance disk size to proceed with the installation.

     ERROR: Insufficient HDD size, Please upgrade the VM HDD size to minimum 500 GB to install Log Collector

     To expand the hard disk size for the Junos Space virtual appliance:

     a. Add a 500 GB capacity hard disk on the Junos Space virtual appliance through VMware vSphere client.

     b. Connect to the console of the Junos Space virtual appliance through SSH.

     c. Select **Expand VM Drive Size**.

     d. Enter the admin password and expand /var with 500 GB.

     e. Once /var is expanded, you are prompted for any further HDD expansion. Select **No** to reboot the system.

        NOTE: Junos Space Network Management Platform must be active and functioning. You must be able to log in to the Junos Space Network Management Platform and Security Director user interfaces before attempting to run the integrated Log Collector setup script again.

     f. After the disk size is expanded and Junos Space Network Management Platform and Security Director user interfaces are accessible, run the following command:

        ./Integrated-Log-Collector-xx.xxx.xxx.sh

        For example, **./Integrated-Log-Collector-20.1R1.xxx.sh**

- The installation stops if the following error message is displayed while installing the integrated Log Collector on a JA2500 appliance or virtual appliance. You must disable OpenNMS by following the steps mentioned in the error message to proceed with the installation.

  ERROR: Opennms is running...
  Please try to disable opennms as described below or in document and retry Log Collector installation...
  STEPS: Login to Network Management Platform --> Administration --> Applications
  Right Click on Network Management Platform --> Manage Services -> Select Network Monitoring and click Stop
  Service Status should turn to Disabled

  After OpenNMS is disabled, run the following command:

  ./Integrated-Log-Collector-xx.xxx.xxx.sh

  For example, **./Integrated-Log-Collector-20.1R1.xxx.sh**

When the integrated Log Collector is installed on the JA2500 appliance or virtual appliance, the following message is displayed:

Shutting down system logger: [OK]
Starting jingest ... jingest started.
{"log-collector-node": {"id":376,"ip-address":"x.x.x.x","priority":0,"node-type":
"INTEGRATED","cpu-usage":0,"memory-usage":0, "fabric-id":0,"display-name":
"Integrated","timestamp":0}}

After the installation is complete, a logging node is automatically added in **Administration** > **Logging Management** > **Logging Nodes**.

Configuring Log Collector Using Scripts

You can use the following command to configure Log Collector using script described in Table 10 on page 45.

```
“jnpr-” <TAB>
[root@NWAPPLIANCE25397 ~]# jnpr- jnpr-configure-node jnpr-configure-ntp
jnpr-configure-timezone jnpr-network-script healthcheckOSLC
```

Table 10: Description of the Log Collector Script

Script	Description
jnpr-configure-node	Master script for the node configuration and network settings.
jnpr-configure-ntp	Script for NTP configuration.

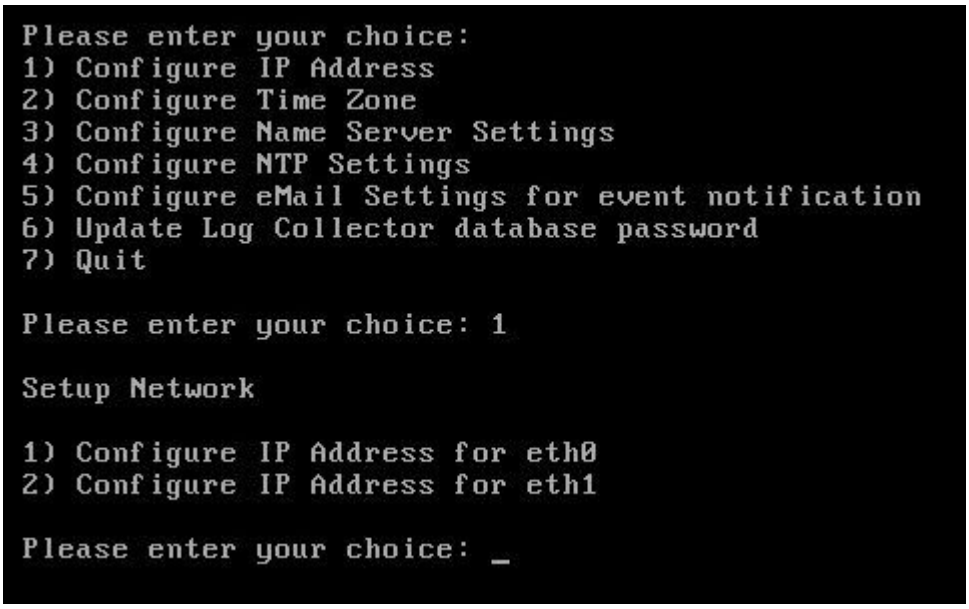
Table 10: Description of the Log Collector Script *(continued)*

Script	Description
jnpr-configure-timezone	Script for time zone configuration.
jnpr-network-script	Script for interface configuration.
healthcheckOSLC	Script for checking the issues with logging infrastructure.

> **NOTE:** You can only configure the IP address of all Log Collector nodes by using the configuration script. If an IP address is configured manually, the Log Collector node cannot be added to Security Director.

Figure 11 on page 46 shows the configuration options.

Figure 11: Configuration Options



NOTE: Starting in Log Collector Release 19.3 onward, the **Update Log Collector database password** option is mandatory in the configuration CLI. Without updating the password you cannot exit the configuration CLI.

When you upgrade a Log Collector application to 19.3 or later and execute **configureNode.sh**, the configuration CLI prompts you to update Log Collector database password. Until the password is updated, you cannot exit the CLI. The password change is required only for the first execution of the **configureNode.sh** script, after successful upgrade of Log Collector application. On subsequent executions of the script it is not mandatory to change the password.

While updating Log Collector database password:

- For All-in-One node setup, the password update will get reflected as soon as you change the password through CLI.
- If you want to setup distributed Log Collector, you can update the Log Collector database password in the receiver through configuration CLI. The update operation will be successful, but to reflect this change in the cluster you need to add at least one storage node. You must add the Log Collector to Security Director only after the password update is reflected in the cluster.
- In an existing distributed Log Collector setup, do not modify the Log Collector database password if no storage nodes are available in the setup, otherwise it will create conflict in the cluster.

Expanding the Size of the VM Disk for Log Collector

You can increase the disk size of your virtual machine (VM) when the log files created by your application become too large.

NOTE: The default shipping configuration of your VM includes 500 GB of disk space.

Before You Begin

- Ensure that the VM is powered off.
- Ensure that the VM has no snapshots.

To expand the disk size using VMware VSphere or VCenter:

1. Deploy the Log Collector VM on a VMware ESX server.

2. Using VSphere client (either the desktop client or the Web), right-click the VM settings.

3. Click **Edit Settings**.

4. Set the Hard disk 2 option to 600. The default disk configuration is 12 GB for hard disk 1 and 500 GB for hard disk 2.

5. Click **Save**.

6. Power on the VM.

To verify and apply the configuration:

1. Log in as a root user from the Log Collector VM.

2. Check the current file system state by entering the **df -h** command.

Filesystem	Size	Used	Available	Use%	Mounted On
/dev/mapper/data1_vg-elasticsearch	500G	267M	500G	1%	/var/lib/elasticsearch

3. Run the */opt/jnpr/bin/resizeFS.sh* script.

   You see the following sample output:

```
[root@LOG-COLLECTOR ~]# /opt/jnpr/bin/resizeFS.sh


Physical volume "/dev/sdb" changed 1 physical volume(s) resized / 0 physical
volume(s) not resized

Extending logical volume elasticsearch to 600.00 GB

Logical volume elasticsearch successfully resized
meta-data=/dev/mapper/data1_vg-elasticsearch isize=256 agcount=4, agsize=32767744
 blks = sectsz=512 attr=2, projid32bit=0 data = bsize=4096 blocks=131070976,
imaxpct=25 = sunit=0 swidth=0 blks naming =version 2 bsize=4096 ascii-ci=0 log
 =internal bsize=4096 blocks=63999, version=2 = sectsz=512 sunit=0 blks,
```

```
lazy-count=1 realtime =none extsz=4096 blocks=0, rtextents=0 data blocks changed
 from 131070976 to 157285376
```

4. Enter the **df -h** command again. Verify the expanded disk space, which should now be 600 GB.

   /dev/mapper/data1_vg-elasticsearch

Filesystem	Size	Used	Available	Use%	Mounted On
/dev/mapper/data1_vg-elasticsearch	600G	267M	600G	1%	/var/lib/elasticsearch

NOTE: You must restart the VM after editing the disk size and then execute the resizeFS.sh script.

For more information on troubleshooting any issue while setting up Log Collector, see the following:

- To learn more about enabling vMotion and fault tolerance logging, see Enabling vMotion and Fault tolerance logging.
- To learn more about VMWare chassis cluster and fault tolerance, see vSphere Availability.
- To learn more about configuring vMotion, see Creating a VMkernel port and enabling vMotion on an ESXi/ESX host and Set Up a Cluster for vMotion.

RELATED DOCUMENTATION

Upgrading Junos Space Network Management Platform | 14

Installing Security Director | 15

Upgrading Security Director | 16

Security Director Log Collector Overview | 28

JSA Log Collector Overview

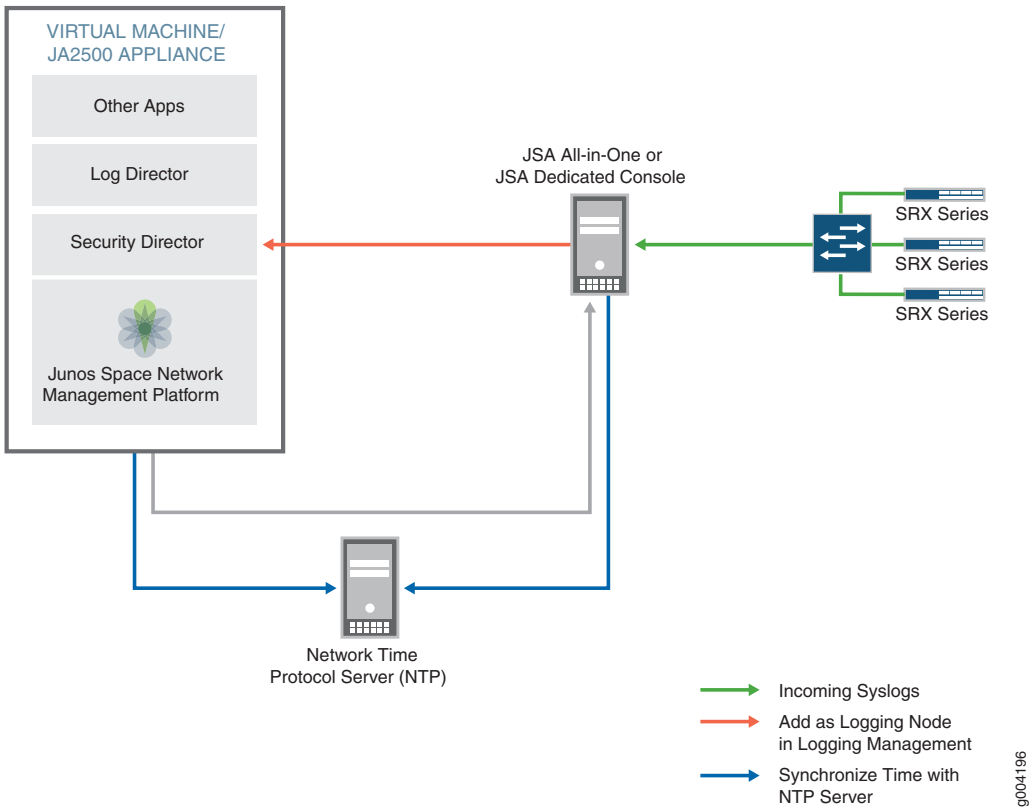
You can use Juniper Secure Analytics (JSA) as a Log Collector to view log data in Security Director. From the JSA console, Security Director queries logs from SRX Series devices. Security Director can use either JSA3800, JSA5800, JSA7500, or virtual JSA for log collection. You must add JSA as a logging node in Security Director to view log data in the Dashboard, Events and Logs, Reports, and Alerts pages.

NOTE: The JSA version supported by Security Director to be added as log collector node is JSA Release 2014.8.R4 or later.

After JSA is deployed, you can configure network devices to send system logs to JSA. It collects the logs in a standalone or clustered setup. For more details on deploying and configuring JSA, see Juniper Secure Analytics documentation.

Figure 12 on page 50 shows the deployment example using the JSA All-in-One or JSA Dedicated Console.

Figure 12: Using JSA All-in-One or JSA Dedicated Console



To add JSA as a logging node in Security Director, see “Adding Log Collector to Security Director” on page 51.

Adding Log Collector to Security Director

You must deploy either Security Director Log Collector or Juniper Secure Analytics (JSA) as a log collector and then add it to Security Director to view the log data in the Dashboard, Events and Logs, Reports, and Alerts pages.

Before You Begin

- Deploy Security Director Log Collector or JSA as a Log Collector.
- Configure system log and security logging for the devices managed by Junos Space Security Director from **Devices** > **Security Devices** > **Modify Configuration**.
- While adding SRX firewall as a log source in JSA or QRadar, set the log source type to Juniper Junos Platform and not Juniper SRX Series Services Gateway.
- You must have the recent version of Juniper Junos Device Support Module (DSM) installed on JSA or QRadar.
- After upgrading Log Collector, database password will reset to default credentials, that is, admin/juniper123. You must re-configure the database password after Log Collector upgrade before adding the Log Collector node to Security Director.

To add Log Collector to Security Director:

1. From the Security Director user interface, select **Administration** > **Logging Management** > **Logging Nodes**, and click the plus sign (+).

   The Add Logging Node page appears.

2. Choose the Log Collector type as **Security Director Log Collector** or **Juniper Secure Analytics**.

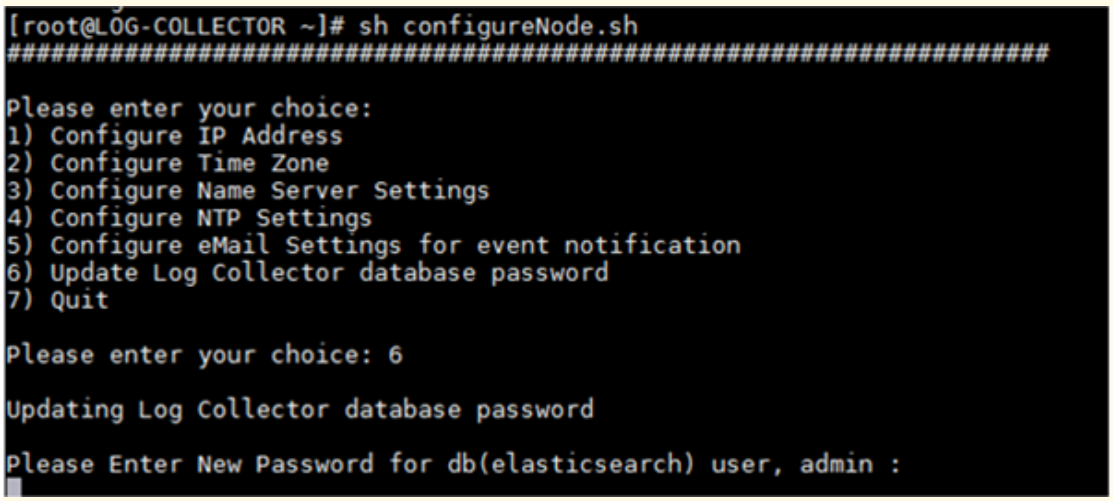
3. Click **Next**.

4. Complete the configuration for Add Collector/JSA Node.

NOTE: From Junos Space Security Director Release 17.2, for distributed Log Collector deployment, you must add only Log Receiver node.

CAUTION: For Security Director Log Collector, provide the default credentials: Username is admin and Password is juniper123. You must change the default password using the Log Collector CLI **configureNode.sh** command as shown in Figure 13 on page 52.

Figure 13: Change Password



For JSA, provide the admin credentials that is used to log in to the JSA console.

5. Click **Next**.

   The certificate details are displayed.

6. Click **Finish**.

7. Review the summary of configuration changes from the summary page and click **Edit** to modify the details, if required.

8. Click **OK** to add the node.

   A new logging node with your configuration is added. To verify that the node is configured correctly, click **Logging Management** to check the status of the node.

To remove an existing Security Director Log Collector and add JSA as a Log Collector:

1. Select **Administration** > **Logging Management** > **Logging Nodes**.
2. Select the existing Security Director Log Collector and click the delete icon to delete Security Director Log Collector node.
3. Click the **+** icon to add JSA as a Log Collector.
4. Configure the SRX Series devices to stop sending logs to Security Director Log Collector, and ensure that logs are sent to the JSA node.

RELATED DOCUMENTATION

Security Director Log Collector Overview | **28**

Setting Up Security Director Log Collector | **34**

JSA Log Collector Overview | **50**

Upgrading Security Director Log Collector

IN THIS SECTION

- Upgrading Log Collector VM or JA2500 Appliance | **54**
- Upgrading Log Collector VM or JA2500 Appliance | **56**
- Upgrading Log Collector CentOS Version from 6.5 to 6.8 | **58**
- Upgrading Integrated Log Collector | **59**
- Upgrading Integrated Log Collector | **59**

NOTE: You must use 20.1R1 Log Collector builds for Security Director Release 21.1R1. There are no Log Collector builds for 21.1R1 release. When you upgrade Security Director release to 21.1R1, you must use Log Collector 20.1R1.

You can upgrade the Log Collector VM or the JA2500 appliance and integrated Log Collector to a later release.

Before You Begin

- You must delete all the Log Collector nodes from **Security Director** > **Administration** > **Logging Management** > **Logging Nodes**.
- Upgrade to a supported version of Junos Space Network Management Platform Release and then upgrade the Security Director application.

See the following topics for information about upgrading Log Collector:

Upgrading Log Collector VM or JA2500 Appliance

NOTE: Create a back up of Log Collector.

Table 11: Log Collector Upgrade Path

Upgrading to Release	Upgrade Path
Log Collector 20.1R1	• Log Collector 19.3R1 > Log Collector 20.1R1 • Log Collector 19.4R1 > Log Collector 20.1R1 You can now perform direct upgrade to 20.1R1 from earlier versions of Junos Space Security Director Release 19.1R1 and 19.2R1. • 19.1R1 > 20.1R1 • 19.2R1 > 20.1R1 **NOTE:** You can perform direct upgrade only for Junos Space Security Director. However, you must follow all the supported upgrade paths for Junos Space Network Management Platform and Log Collector to upgrade to 20.1R1.
Log Collector 19.4R1	• Log Collector 19.2R1 > Log Collector 19.4R1 • Log Collector 19.3R1 > Log Collector 19.4R1
Log Collector 19.3R1	• Log Collector 19.2R1 > Log Collector 19.3R1 • Log Collector 19.1R2 > Log Collector 19.3R1 • Log Collector 19.1R1 > Log Collector 19.3R1

Table 11: Log Collector Upgrade Path *(continued)*

Upgrading to Release	Upgrade Path
Log Collector 19.2R1	• Log Collector 19.1R2 > Log Collector 19.2R1 • Log Collector 19.1R1 > Log Collector 19.2R1 • Log Collector 18.4R1 > Log Collector 19.2R1
Log Collector 19.1R2	• Log Collector 19.1R1 > Log Collector 19.1R2 • Log Collector 18.4R1 > Log Collector 19.1R2 • Log Collector 18.3R1 > Log Collector 19.1R2
Log Collector 19.1R1	• Log Collector 18.4R1 > Log Collector 19.1R1 • Log Collector 18.3R1 > Log Collector 19.1R1 You can now perform direct upgrade to 19.1R1 from earlier versions of Log Collector Release 18.2R1, 18.1R1, and 17.2R2. • 18.2R1 > 19.1R1 • 18.1R1 > 19.1R1 • 17.2R2 > 19.1R1 **NOTE:** You can perform direct upgrade only for Junos Space Security Director and Log Collector. However, you must follow all the supported upgrade paths for Junos Space Network Management Platform to upgrade to 19.1R1.

To upgrade Log Collector VM or JA2500 Appliance:

1. Download the Log Collector upgrade script from the download site.

2. Use the **ssh** command to log in to the Log Collector node.

3. Copy the upgrade script to the /root directory of all the nodes that you want to upgrade.

4. Change the file permission using the following command:

   chmod +x Log-Collector-Upgrade-xx.xxx.xxx.sh

   For example, **chmod +x Log-Collector-Upgrade-20.1R1.xxx.sh**

5. Run the upgrade script using the **./Log-Collector-Upgrade-xx.xxx.xxx.sh** command.

   For example, **./Log-Collector-Upgrade-20.1R1.XXX.sh**

The status of the upgrade is shown on the console.

6. Add the logging nodes back to Security Director from **Security Director** > **Administration** > **Logging Management** > **Logging Nodes**.

   See “Adding Log Collector to Security Director” on page 51.

Upgrading Log Collector VM or JA2500 Appliance

> **NOTE:**
> - Starting in Security Director Release 19.3R1, Centos upgrade from 6.5 to 6.8 is supported in Log Collector. To upgrade the CentOS, see “Upgrading Log Collector CentOS Version from 6.5 to 6.8” on page 58.

To upgrade Log Collector All-In-One node:

1. Download the Log Collector upgrade script **Log-Collector-Upgrade-20.1R1.X.sh** from the download site.

2. Copy the Log Collector upgrade script to the Log Collector All-In-One node.

3. Connect to the CLI Log Collector All-In-One node.

4. Navigate to the location where you have copied Log Collector upgrade script.

5. Run Log Collector upgrade script.

   sh Log-Collector-Upgrade-20.1R1.X.sh

6. Select from the below options and continue.

   1) Upgrade WITHOUT Recovering current log data

   [This will PERMANENTLY DELETE THE CURRENT LOG DATA]

   2) Upgrade and Recover the current log data

   3) Exit

   Is this running on SSD? [Y/N]

   Wait for the upgrade to complete.

To upgrade distributed Log Collector:

Before You Begin

- For upgrade process, you should be able to ping both Log Receiver and Log Storage nodes.
- Download the Log Collector upgrade script **Log-Collector-Upgrade-20.1R1.X.sh** from the download site.
- Copy the Log Collector upgrade script to Log Receiver and Log Storage nodes of the distributed deployment.

To upgrade on Log Receiver node:

1. Connect to the Log-Receiver Node CLI.

2. Navigate to the location where you have Log Collector upgrade script.

3. Run Log Collector upgrade script:

   sh Log-Collector-Upgrade-20.1R1.X.sh

4. Select from the below options and continue.

   Please choose how you want to upgrade Log Collector:

   1) Upgrade WITHOUT Recovering current log data.

   [This will PERMANENTLY DELETE THE CURRENT LOG DATA]

   2) Upgrade and Recover the current log data

   3) Exit

To upgrade on Log Storage node:

1. Run Log Collector upgrade script:

   sh Log-Collector-Upgrade-20.1R1.X.sh

2. Enter the Log Receiver Node IP.

3. Select from the below options and continue

   Please choose how you want to upgrade Log Collector:

   1) Upgrade WITHOUT Recovering current log data.

   [This will PERMANENTLY DELETE THE CURRENT LOG DATA]

   2) Upgrade and Recover the current log data

3) Exit

Upgrading Log Collector CentOS Version from 6.5 to 6.8

To upgrade CentOS version:

1. Download CentOS upgrade script and ISO image from download site to**/tmp** directory in Log Collector virtual machine.

2. Run the following command

   Chmod +x CentOS-Upgrade-20.1R1.31.sh

3. Run the script by providing the ISO image as argument.

   ./CentOS-Upgrade-20.1R1.31.sh log-collector-iso-20.1R1.13.iso

4. Run “upgrade” or “recovery and then upgrade”. The recovery and then upgrade should be performed only when the last upgrade has failed or was interrupted due to power failure.

5. Reboot Log Collector, after the upgrade is successful.

   NOTE:
   - The upgrade is supported from CentOS version 6.5 to 6.8 only.
   - For running the upgrade script, use console or telnet (for appliances) and do not use ssh session or any other remote access mechanisms.

6. Verify if the upgrade is successful by running the commands in the console.

   The commands and the expected results are given below:

   # uname -a

   Linux LOG-COLLECTOR 2.6.32-754.18.2.el6.x86_64#1 SMP Wed Aug 14 16:26:59 UTC 2019 x86_64 x86_64 x86_64/Linux

   # cat/etc/redhat-release

   CentOS release 6.8 (Final)

Upgrading Integrated Log Collector

To upgrade an integrated Log Collector to a latest release:

1. Download the integrated Log Collector script from the download site.
2. Copy the integrated Log Collector script to a JA2500 appliance or virtual appliance.
3. Connect to the CLI of a JA2500 appliance or virtual appliance with admin privileges.
4. Navigate to the location where you have copied the integrated Log Collector script.
5. Change the file permission using the following command:

   chmod +x Integrated-Log-Collector-xx.xxx.xxx.sh

   For example, **chmod +x Integrated-Log-Collector-20.1R1.xxx.sh**
6. Run the integrated Log Collector script using the following command:

   ./Integrated-Log-Collector-xx.xxx.xxx.sh

   For example, **./Integrated-Log-Collector-20.1R1.xxx.sh**

NOTE:

- The integrated Log Collector does not support high availability (HA) even if it is installed in a Junos Space HA cluster. The integrated Log Collector must be installed only on one of the Junos Space cluster nodes.
- 500 eps is supported for the integrated Log Collector.

Upgrading Integrated Log Collector

1. Copy **Integrated-Log-Collector-20.1R1.x.sh** to the space node.
2. Run the script: **sh Integrated-Log-Collector-20.1R1.x.sh**
3. Select from following options and continue:

   Please choose how you want to upgrade Log Collector:

1) Upgrade WITHOUT Recovering current log data.

[This will PERMANENTLY DELETE THE CURRENT LOG DATA]

2) Upgrade and Recover the current log data.

3) Exit

NOTE: After upgrading Log Collector, database password will reset to default credentials, that is, admin/juniper123. You must re-configure the database password after Log Collector upgrade before adding the Log Collector node to Security Director.

After upgrading the log collector, add the log collector node. See "Adding Log Collector to Security Director" on page 51.

For Security Director log collector, provide the default credentials admin/juniper123. You must change the default password.

For JSA, provide the admin credentials that is used to log in to the JSA console.

RELATED DOCUMENTATION

Upgrading Junos Space Network Management Platform | 14

Upgrading Security Director | 16