JUNIPER NETWORKS

Security Director

Security Director Installation and Upgrade Guide

Modified: 2017-08-31

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

Security Director Security Director Installation and Upgrade Guide

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 http://www.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Figures

List of Tables

About the Documentation

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 http://www.juniper.net/techpubs/.

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 http://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

- JA2500

Documentation Conventions

Table 1 on page x 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 x 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*
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*

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

Convention	Description	Examples
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		
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, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at http://www.juniper.net/techpubs/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 J-Care or Partner Support Service 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 http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://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: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- 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 http://www.juniper.net/support/requesting-support.html.

CHAPTER 1

Installing and Upgrading Security Director

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—For details about setting up a JA2500 appliance for Security Director, see "Setting Up a JA2500 Appliance for Security Director" on page 16.

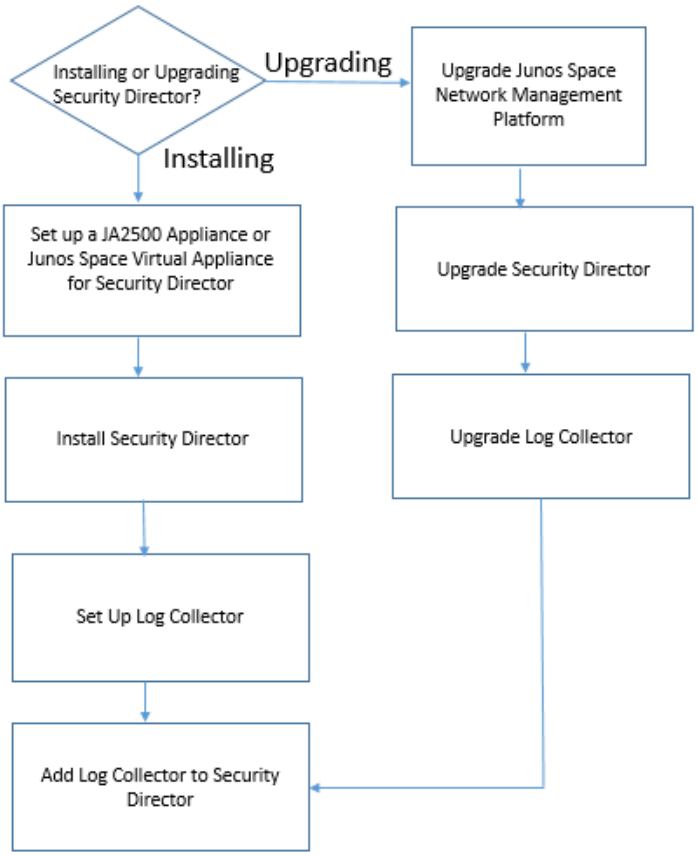
  For details about the JA2500 appliance and instructions for installation, see the Juniper Networks JA2500 Junos Space Appliance Hardware Guide.

- Junos Space Virtual Appliance—For details about setting up a Junos Space virtual appliance for Security Director, see "Setting Up a Junos Space Virtual Appliance for Security Director" on page 17.

  For details about installing Junos Space virtual appliances, see the Junos Space Virtual Appliance Installation and Configuration Guide.

Figure 1 on page 16 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 on page 16
- Setting Up a Junos Space Virtual Appliance for Security Director on page 17

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.

Configuring Basic Settings for a JA2500 Appliance

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 on page 15

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.

Configuring the Basic Settings for a Junos Space Virtual Appliance

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 on page 15

Upgrading Junos Space Network Management Platform

Junos Space Security Director release is supported only on the corresponding Junos Space Network Management Platform release. For example, Security Director Release 17.1R1 is supported only on Junos Space Network Management Platform Release 17.1R1. If your appliance is running the supported version of Junos Space, you can skip this procedure and begin installation of Security Director.

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 17.1R1.

NOTE: If the Junos Space Platform installation is running a version earlier than Release 16.1, you must first upgrade the installation to Release 16.1R2 and then upgrade to Release 17.1R1. For upgrade details, see Upgrading to Junos Space Network Management Platform Release 16.1R1.

NOTE: For 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 on page 16
- Setting Up a Junos Space Virtual Appliance for Security Director on page 17

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 17.

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 on page 17
- Upgrading Security Director on page 19
- Setting Up Security Director Log Collector on page 30

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.
- 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 17.
- The Junos Space Network Management Platform should be active and functioning.

Upgrade Information

Upgrading to Security Director 17.1R1

You can upgrade to Junos Space Network Management Platform Release 17.1R1 and Security Director Release 17.1R1 from the following releases:

- Junos Space Network Management Platform Release 16.1R2 and Security Director Release 16.2R1
- Junos Space Network Management Platform Release 16.1R1 and Security Director Release 16.1R1

Upgrading to Security Director 16.2R1

You can upgrade to Junos Space Network Management Platform Release 16.1R2 and Security Director Release 16.2R1 from the following releases:

- Junos Space Network Management Platform Release 16.1R1 and Security Director Release 16.1R1
- Junos Space Network Management Platform Release 15.2R2 and Security Director Release 15.2R2

Upgrading to Security Director 16.1R1

You can upgrade to Junos Space Network Management Platform Release 16.1R1 and Security Director Release 16.1R1 from the following releases:

- Junos Space Network Management Platform Release 15.2R2 and Security Director Release 15.2R2
- Junos Space Network Management Platform Release 15.2R1 and Security Director Release 15.2R1

Upgrade to Security Director 15.2R2

You can upgrade to Junos Space Network Management Platform Release 15.2R2 and Security Director Release 15.2R2 from the following release:

- Junos Space Network Management Platform Release 15.2R1 and Security Director Release 15.2R1

NOTE:

- Security Director 15.2R2 does not support the Integrated Log Collector VM.
- Data migration from an earlier version of Log Collector to a later version is not supported.

Upgrade to Security Director 15.2R1

You can upgrade to Junos Space Network Management Platform Release 15.2R1 and Security Director Release 15.2R1 from the following releases:

- Junos Space Network Management Platform Release 15.1R1 and Security Director Release 15.1R1
- Junos Space Network Management Platform Release 15.1R2 and Security Director Release 15.1R2

Procedure

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.

   Perform the following steps before upgrading from Security Director Release 15.2R1 or 15.2R2 to Security Director Release 16.1R1 or Security Director Release 15.2R2 to Security Director Release 16.2R1:

   a. Back up Junos Space Security Director Release that you want to upgrade. See Executing the Data Back Up Procedure.

b. Upgrade to the supported Junos Space Network Management Platform release, and restore the backup.

NOTE: Starting in Junos Space Security Director Release 16.2R1, all IPS report definitions are consolidated into a single report definition called IPS Report. After upgrading Security Director to 16.2R1, IPS reports for already scheduled IPS report definitions will not be generated because the individual IPS report definitions do not exist. You must use the consolidated IPS report.

Release History Table

Release	Description
16.2	Starting in Junos Space Security Director Release 16.2R1, all IPS report definitions are consolidated into a single report definition called IPS Report.

Related Documentation

- Upgrading Junos Space Network Management Platform on page 17
- Installing Security Director on page 18

CHAPTER 2

Setting Up and Upgrading Log Collector

Security Director Log Collector Overview

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

In Junos Space Security Director Release 15.2R1, you can set up Log Collectors in a VM environment. From Junos Space Security Director Release 15.2R2, you can set up Log Collectors in a VM and JA2500 environment.

For easy scaling, begin with a single Log Collector and incrementally add dedicated Log Collectors, as your needs expand. You must configure a Log Indexer if you are using more than one Log Collector. For a VM environment, a single OVA image is used to deploy the Log Collector and Log Indexer. The image presents a configuration script after you log in. During setup, you can configure the node as either a Log Collector or a Log Indexer. At deployment, the user must select appropriate memory and CPU configuration values.

Table 3: Log Collector Setup Environment

Release	Option
15.2R1	VM
15.2R2 and later releases	VM, JA2500

NOTE: In Security Director Release 15.2R1, Log Collector is supported only as a VM that can be deployed on VMWare ESX server.

From Security Director Release 16.1R1, you can configure Log Collector as an All-in-One node or an 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.

Table 4 on page 24 describes the supported Log Collector node types in various releases.

Table 4: Supported Log Collector Node Types

Node Type	Release 15.2R1 and 15.2R2	From Release 16.1R1
All-in-One node	Yes	Yes
Log Receiver node	Yes	Yes
Log Storage node	Yes (Log Indexer node)	Yes
Query node	Yes (20K)	No
Master node	Yes (20K)	No
Integrated node	No	Yes

NOTE: You can configure eth0 or eth1 for receiving logs from devices in different Log Collector deployment modes.

NOTE: Starting in Junos Space Security Director Release 16.2R1, you can use JSA as a Log Collector node. See "JSA Log Collector Overview" on page 44 and "Adding Log Collector to Security Director" on page 45.

NOTE: High Availability is not supported on Security Director Log Collector. However, JSA as Log Collector supports High Availability.

NOTE: Security Director Logging and Reporting is not supported on JA1500 appliance.

- Log Director on page 25
- Log Collector Deployment Modes on page 25
- Log Collector Storage Requirements on page 26
- Deploying Log Collector as an All-in-One Node on page 26

- Deploying Multiple Log Collectors on page 27
- Deploying Log Collector as an Integrated Node on page 29

Log Director

Log Director is a plug in on the Junos Space Network Management Platform, which is used for system log data collection for SRX and vSRX Series devices running Junos OS. Log Director consists of two components:

- Junos Space plug in application
- VM or JA2500 deployment of Log Receiver and Log Storage nodes

Log Collector Deployment Modes

Table 5 on page 25 and Table 6 on page 25 describe different modes in which Log Collector can be deployed.

Table 5: Log Collector Deployment Modes for Security Director Release 15.2

Node Type	Description
All-in-One Node (Combined deployment)	Both the Log Receiver and Log Indexer nodes run on the same VM. It supports up to 2,000 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. SRX Series devices must be configured with the Log Receiver node IP address to send system logs. Upon configuration, this node parses and forwards logs to Log Indexer node. You must provide the IP address of the Log Indexer node when configuring this node.
Log Indexer Node (Distributed deployment)	This node analyzes, indexes, and stores the system logs. It receives the system logs from Log Receiver node and serves all the queries from Security Director. The Log Indexer node roles are split into the following three major roles when the scale of deployment is more than 10K eps: • Log Storage node: Dedicated node for storing the indexed system logs. • Master node: Dedicated cluster manager node that monitors and maintains the integrity of Log Indexer cluster. • Query node: Dedicated query node that receives system logs from Log Receiver node(s) and distributes them across the available log storage nodes. Also, this node acts as the single query point for the Security Director application and responds to all the system log queries.

Table 6: Log Collector Deployment Modes for Security Director Release 16.1 and Later

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.

Table 6: Log Collector Deployment Modes for Security Director Release 16.1 and Later *(continued)*

Node Type	Description
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:**

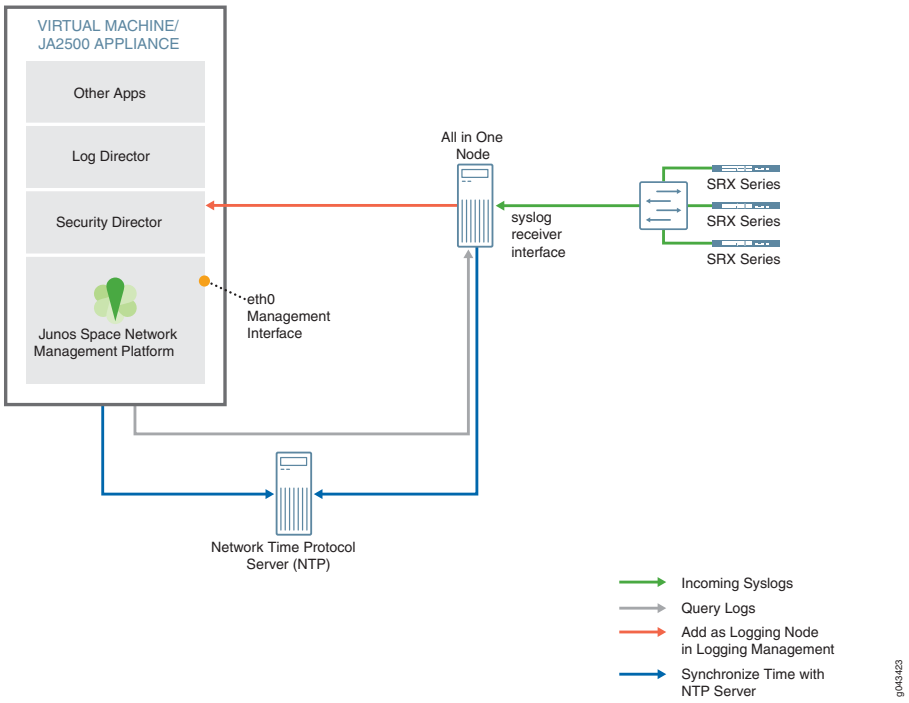
- **Time-based rollover—Logs that are older than 45 days are automatically rolled over, even if the disk space is available.**
- **Disk size-based rollover—Older logs get rolled over when the disk size reaches 400 GB.**

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 2 on page 27 shows an example of an All-in-One node deployment.

Figure 2: 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 3 on page 28 shows the deployment example using multiple nodes for up to 10K eps.

Figure 3: Using Multiple Nodes for Up to 10K eps

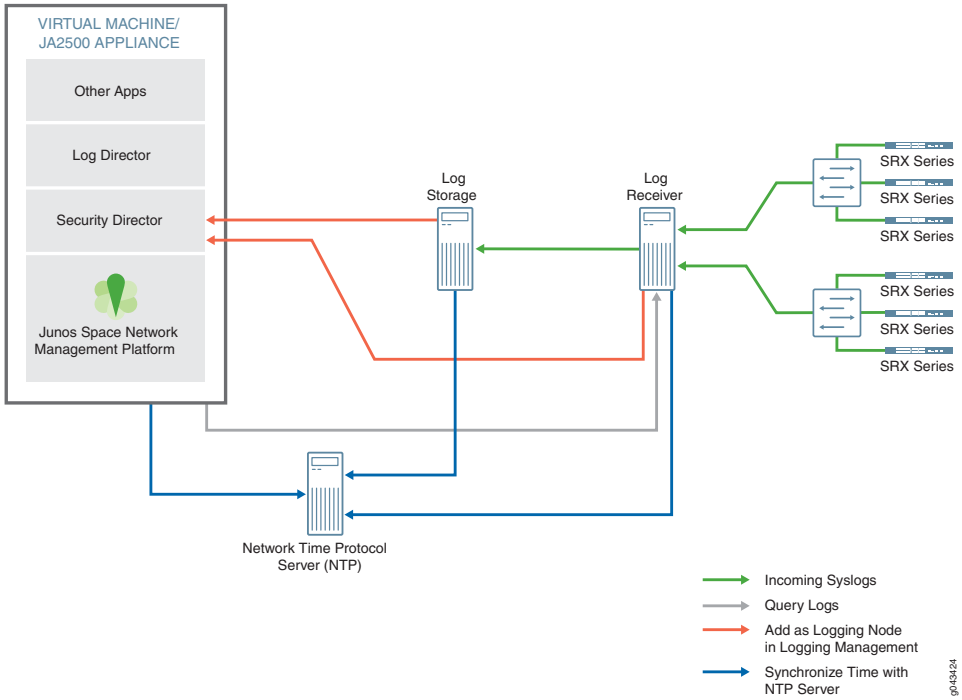
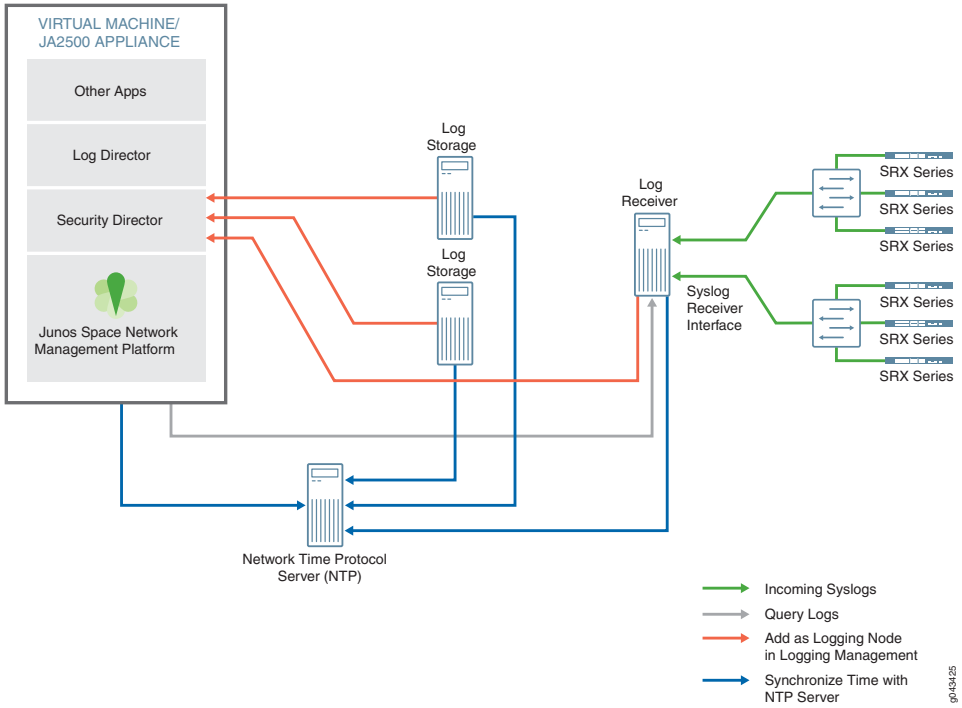


Figure 4 on page 29 shows the deployment example using multiple nodes for greater than 10K eps.

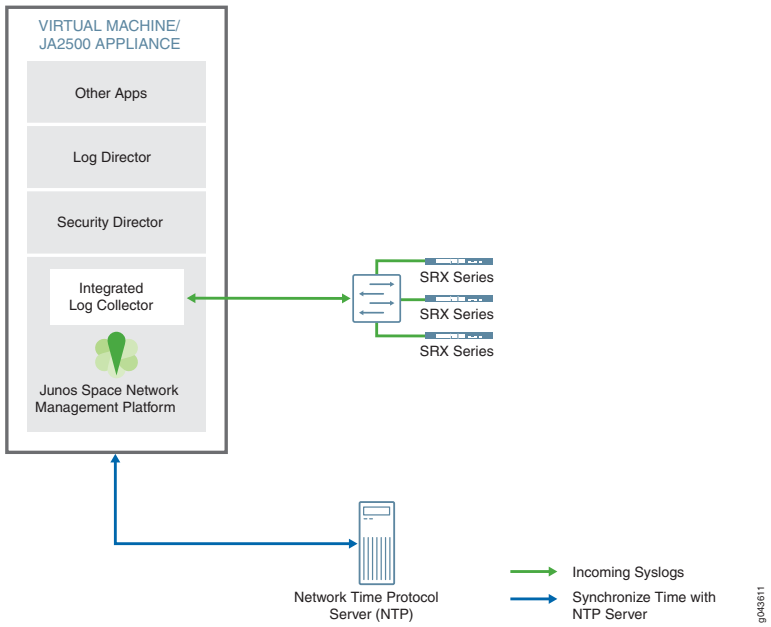
Figure 4: Using Multiple Nodes for Greater Than 10K eps



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.

Figure 5: Integrated Node Deployment



Related Documentation

- Upgrading Junos Space Network Management Platform on page 17
- Installing Security Director on page 18
- Upgrading Security Director on page 19
- Setting Up Security Director Log Collector on page 30

Setting Up Security Director Log Collector

A single Security Director image installs Security Director, Log Director, and Security Director Logging and Reporting applications.

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)—Used for communication between the Junos Space server and the Log Collector node agent.
  - Port 8003 (TCP)—Used for log data queries.
  - Port 9200 (TCP)—Used in Log Storage nodes.
  - Port 9300 (TCP)—Used for communicating across elasticsearch cluster.

  - Port 4567 (TCP)—Used for communication between the Log Receiver node and Log Storage node.
  - Port 514 (TCP)—Used for receiving system logs.
  - Port 514 (UDP)—Used for receiving system logs.
  - Port 22 (TCP)—Used for SSH connectivity.
- 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)

- Specifications for Deploying a Log Collector Virtual Machine on a VMware ESX Server on page 31
- Deploying Log Collector VM on a VMWare ESX Server on page 33
- Deploying Log Collector VM on a KVM Server on page 34
- Deploying Log Collector on a JA2500 Appliance on page 36
- Installing Integrated Log Collector on a JA2500 Appliance or Junos Space Virtual Appliance on page 38
- Configuring Log Collector Using Scripts on page 41
- Expanding the Size of the VM Disk for Log Collector on page 42

Specifications for Deploying a Log Collector Virtual Machine on a VMware ESX Server

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 on a VMware ESX server with Solid State Drives (SSD) and the VM configuration on a VMware ESX server with non Solid State Drives for different Security Director Releases. They list the required specifications for deploying a Log Collector VM on a VMware ESX server for various sustained 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 7: VMware ESX Server with Solid State Drives (SSD) for Security Director Release 15.2R1 and 15.2R2

Setup	Log Receiver Node			Log Indexer Node			Log Query Node		Cluster Manager Node		Total Nodes
	Number of Nodes	CPU	Memory	Number of Nodes	CPU	Memory	CPU	Memory	CPU	Memory	
4K eps	1	4	16 GB	-	-	-	-	-	-	-	1

Table 7: VMware ESX Server with Solid State Drives (SSD) for Security Director Release 15.2R1 and 15.2R2 *(continued)*

Setup	Log Receiver Node			Log Indexer Node			Log Query Node		Cluster Manager Node		Total Nodes
	Number of Nodes	CPU	Memory	Number of Nodes	CPU	Memory	CPU	Memory	CPU	Memory	
7K eps	1	4	16 GB	1	4	32 GB	-	-	-	-	2
10K eps	2	8	32 GB	1	8	32 GB	-	-	-	16 GB	2
20K eps	2	16	32 GB	3	16	32 GB	8	16 GB	4	16 GB	6

Table 8: VMware ESX Server with Non Solid State Drives (SSD) for Security Director Release 15.2R1 and 15.2R2

Setup	Log Receiver Node			Log Indexer Node			Log Query Node		Cluster Manager Node		Total Nodes
	Number of Nodes	CPU	Memory	Number of Nodes	CPU	Memory	CPU	Memory	CPU	Memory	
2K eps	1	4	16 GB	-	-	-	-	-	-	-	1
5K eps	1	8	16GB	1	4	32 GB	-	-	-	-	2
10K eps	2	8	32 GB	1	8	32 GB	-	-	-	16 GB	3
20K eps	2	16	32 GB	4	16	32 GB	8	16 GB	4	16 GB	8

Table 9: VMware ESX Server with Solid State Drives (SSD) for Security Director Release 16.1 and Later

Setup	Log Receiver Node			Log Storage Node			Total Nodes
	Number of Nodes	CPU	Memory	Number of Nodes	CPU	Memory	
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 10: VMware ESX Server with Non-Solid State Drives for Security Director Release 16.1 and Later

Setup	Log Receiver Node			Log Storage Node			Total Nodes
	Number of Nodes	CPU	Memory	Number of Nodes	CPU	Memory	
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).

   NOTE: For Security Director Release 15.2R1 and 15.2R2, see Table 7 on page 31 and Table 8 on page 32. For Security Director Release 16.1R1 and later see Table 9 on page 32 and Table 10 on page 33.

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 root 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 45.

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

Starting in Security Director Release 15.2R2, you can deploy Log Collector VM on a kernel-based virtual machine (KVM) server installed on CentOS Release 6.5.

Before You Begin

- The KVM server and supported packages must be installed on a machine running CentOS Release 6.5 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.

Procedure

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 45.

Deploying Log Collector on a JA2500 Appliance

Starting in Security Director Release 15.2R2, 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.

Create a Bootable USB Flash Drive

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.

Install Log Collector Using a USB Flash Drive

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 root password when prompted.

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 45.

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

Starting in Security Director Release 16.1R1, 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.

NOTE: **Integrated Log Collector on a JA2500 appliance or Junos Space virtual appliance supports only 500 eps.**

Before You Begin

The prerequisites for installing an integrated Log Collector on a JA2500 appliance or virtual appliance are as follows:

- 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.

Specifications

Table 11 on page 39 shows the specifications for installing the integrated Log Collector on a JA2500 appliance.

Table 11: 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.
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 12 on page 39 shows the specifications for installing the integrated Log Collector on Junos Space virtual appliance.

Table 12: 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.

Procedure

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-17.1R1.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-17.1R1.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-17.1R1.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-17.1R1.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 13 on page 41.

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

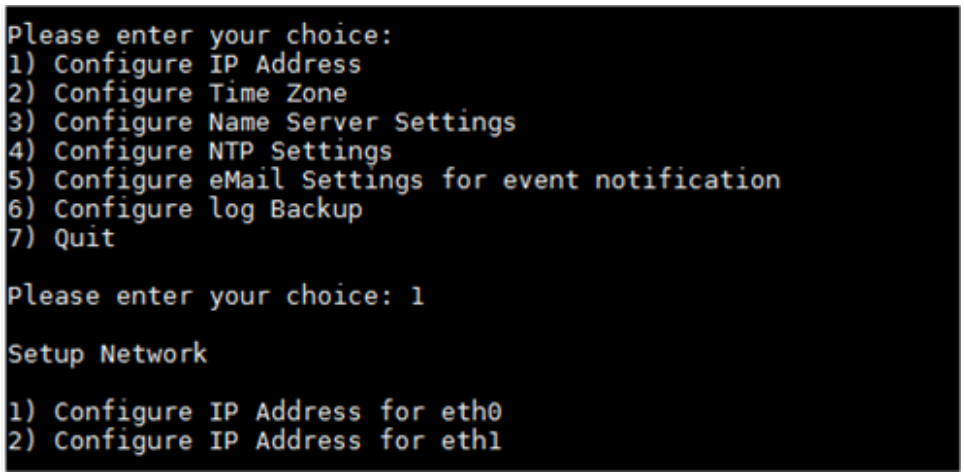
Table 13: Description of the Log Collector Script

Script	Description
jnpr-configure-node	Master script for the node configuration and network settings.
jnpr-configure-ntp	Script for NTP configuration.
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 6 on page 42 shows the configuration options.

Figure 6: Configuration Options



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.

Configuring the Disk Capacity

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.

Verifying and Applying 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.

Release History Table

Release	Description
16.1	Starting in Security Director Release 16.1R1, you can install an integrated Log Collector on a JA2500 appliance or Junos Space virtual appliance.
15.2R2	Starting in Security Director Release 15.2R2, you can deploy Log Collector VM on a kernel-based virtual machine (KVM) server installed on CentOS Release 6.5.

Related Documentation

- Upgrading Junos Space Network Management Platform on page 17
- Installing Security Director on page 18
- Upgrading Security Director on page 19
- Security Director Log Collector Overview on page 23

JSA Log Collector Overview

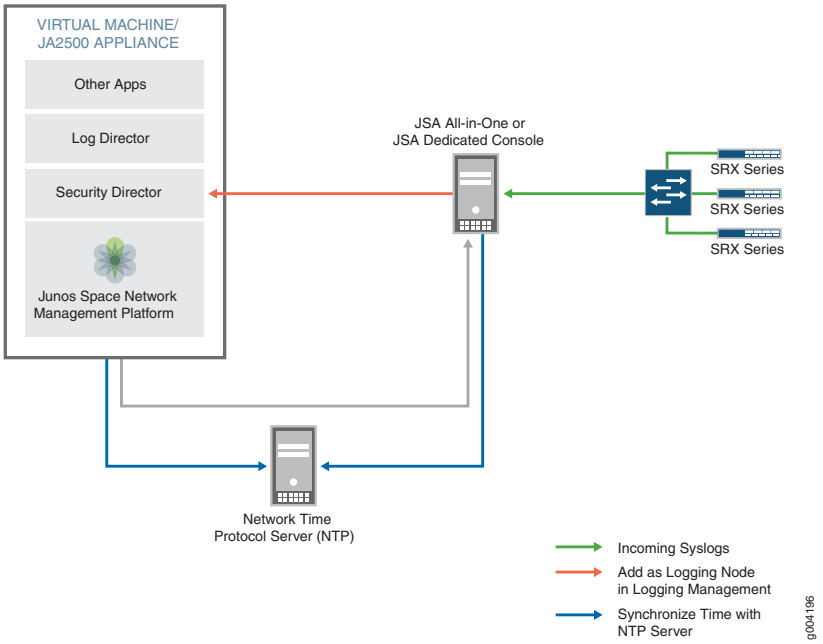
Starting in Security Director Release 16.2 R1, you can use Juniper Secure Analytics (JSA) as a Log Collector to view log data in Security Director. From the JSA console, Security Director queries logs from SRX Series devices. Security Director can use either JSA3800, JSA5800, JSA7500, or virtual JSA 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 SD 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 7 on page 45 shows the deployment example using the JSA All-in-One or JSA Dedicated Console.

Figure 7: 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 45.

Release History Table

Release	Description
16.2	Starting in Security Director Release 16.2 R1, you can use Juniper Secure Analytics (JSA) as a Log Collector to view log data in Security Director.

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**.

Procedure

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**.

   If you select **Security Director Log Collector**, then you must also select the deployment.

3. Click **Next**.

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

   NOTE: **Provide the root credentials for the Security Director Log Collector node. For JSA, provide the admin credentials that is used to log in to the JSA console.**

5. If the Log Collector type is Security Director Log Collector, then **Add Another Node** is displayed. Add multiple nodes as needed.

6. Click **Next**.

   The certificate details are displayed.

7. Click **Finish**.

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

9. 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.

Removing Security Director Log Collector and Adding JSA as a Log Collector

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.

   You can either add All-in-One node for the standalone deployment, or Console node for the distributed deployment.

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 on page 23
- Setting Up Security Director Log Collector on page 30
- JSA Log Collector Overview on page 44

Upgrading Security Director Log Collector

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.

- Upgrading Log Collector from 15.2R1 to 15.2R2 on page 47
- Upgrading Log Collector VM or JA2500 Appliance from 15.2R2 or Later Releases on page 48
- Upgrading Integrated Log Collector on page 49

Upgrading Log Collector from 15.2R1 to 15.2R2

NOTE: **The supported upgrade path is Log Collector 15.2R1 > Log Collector 15.2R2.**

To upgrade from Log Collector 15.2R1 to Log Collector 15.2R2:

1. Download the Log Collector upgrade image for VM from the download site.

2. Copy the rpm file **nwscripts-1-2.noarch.12.rpm** to each Log Receiver node, Log Indexer, or Log Receiver and Indexer node.

3. Upgrade each Log Receiver node, Log Indexer node, or Log Receiver and Indexer node using the **rpm –Uvh nwscripts-1-2.noarch.12.rpm** command.

NOTE: Upgrading Log Collector from 15.1 to Log Collector 15.2R1 is not supported.

Upgrading Log Collector VM or JA2500 Appliance from 15.2R2 or Later Releases

NOTE: Create a back up of Log Collector Release 15.2R2.

NOTE:

The supported upgrade path to Log Collector 16.1R1, 16.2R1, and 17.1R1 are:

- The upgrade path to Log Collector 17.1R1:
  - Log Collector 15.2R2 > Log Collector 16.1R1/16.2R2 > Log Collector 17.1R1
- The upgrade path to Log Collector 16.2R1:
  - Log Collector 15.2R2 > Log Collector 16.1R1 > Log Collector 16.2R1
  - Log Collector 15.2R2 > Log Collector 16.2R1
- The upgrade path to Log Collector 16.1R1:
  - Log Collector 15.2R2 > Log Collector 16.1R1

1. If you had changed the log database password for the logging nodes in Log Collector Release 15.2R2, perform the following steps. Otherwise, continue with Step 2.

   NOTE: This step is applicable from Release 15.2R2 to 16.1R1.

   a. Use the **ssh** command to log in to the node.

   b. Open the **elasticsearch.yml** file located at */etc/elasticsearch/* in a text editor.

   c. In the **elasticsearch.yml** file, search for http.basic.password and replace the changed password with *58dd311734e74638f99c93265713b03c391561c6ce626f8a745d1c7ece7675fa*

   d. Save the changes.

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

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-17.1R1.xxx.sh**

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

   For example, **./Log-Collector-Upgrade-17.1R1.XXX.sh**

   The status of the upgrade is shown on the console.

   NOTE:
   - From release 16.2R1, the **Logstash** process no longer runs on the Log Receiver node. Instead, the **jingest** process will run.
   - You must ensure that the **jingest** and **elasticsearch** processes are running.

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 45.

NOTE: For upgrading from 15.2R2 to 16.1R1:

- Multiple-node deployment is a combination of Log Receiver and Log Storage nodes. You can add a maximum of one Log Receiver node and three Log Storage nodes.
- Only one Log Receiver node is supported for all levels of deployment. If you have multiple Log Receivers in the Release 15.2R2 setup, upgrade only one Log Receiver to Release 16.2R1 and delete the other Log Receivers.
- Log Query node and Master node are not supported. So you can delete them.
- You must run the upgrade script on each node to upgrade it to the corresponding release.

Upgrading Integrated Log Collector

To upgrade an integrated Log Collector to a latest release:

NOTE: Integrated Log Collector is supported from 16.1R1 Release onwards.

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-17.1R1.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-17.1R1.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.

Related Documentation

- Upgrading Junos Space Network Management Platform on page 17
- Upgrading Security Director on page 19