

Junos Space Security Director

Logging and Reporting Getting Started Guide

Release

14.1 R2



Modified: 2016-06-22

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

Copyright © 2016, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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

Junos Space Security Director Logging and Reporting Getting Started Guide

Copyright © 2016, 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 <http://www.juniper.net/support/eula.html>. 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	vii
	Requesting Technical Support	viii
	Self-Help Online Tools and Resources	viii
	Opening a Case with JTAC	viii
Part 1	Overview	
Chapter 1	Logging and Reporting Overview	3
	Understanding Junos Space Security Director Logging and Reporting	3
	Logging	3
	Monitoring	4
	Alert and Notifications	4
	Reports	4
	Understanding Role-Based Access Control	5
Chapter 2	Junos Space Security Director Logging and Reporting	7
	Understanding the Log Collector Deployment Modes	7
	Overview	7
	Specifications for Deploying a Log Collector Virtual Machine on an ESX Server	8
	Specifications for Deploying JA2500 as a Log Collector	9
	Prerequisites for Security Director Logging and Reporting	10
	Installing Junos Space Security Director	10
	Installing Virtual Log Collectors	11
	Installing a JA2500 Log Collector Appliance Image Using a USB Drive	11
	Deploying a Single Log Collector	15
	Deploying Multiple Log Collectors	17
	Adding the Log Collector Subsystem as a Specialized Node	21
	Upgrading the Log Collector	22
Chapter 3	Junos Space Security Director Logging and Reporting on the JA2500 Appliance in an Integrated Environment	23
	Installation Steps Overview	23
	Prerequisites for Installing Junos Space Security Director Logging and Reporting in a JA2500 Appliance	24
	Specifications for Log Collector VM Installation on a JA2500 Appliance	25

	Installing Junos Space Security Director	25
	Installing the Log Collector VM Application on the Junos Space Network Management Platform	26
	Adding the Log Collector Subsystem as a Specialized Node	28
Chapter 4	Log Director	29
	Log Director Overview	29
	Logging	29
	Using Log Messages for Troubleshooting Issues	30
	Log Collectors	31
	Reporting Devices	33
	Global Settings	34
Chapter 5	Security Director and SRX Series Device Settings for Logging	37
	Configuring Security Director and SRX Series Devices to Receive Logs	37
	Configuring Security Logging	37
	Modifying Syslog	40
	Enabling Logging on Branch SRX Series Devices	42
	Enabling Logging on High-End SRX Series Devices	42
Chapter 6	Back Up and Restore Log Collector Data	43
	Log Collector Database Files Overview	43
	Backing Up Log Collector Data	44
	Restoring Log Collector Data	45

About the Documentation

- Documentation and Release Notes on page v
- Documentation Conventions on page v
- Documentation Feedback on page vii
- Requesting Technical Support on page viii

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>.

Documentation Conventions

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

Table 1: Notice Icons







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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>

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.	<ul style="list-style-type: none">To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i>>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	<pre>[edit] routing-options { static { route default { nexthop <i>address</i>; retain; } } }</pre>
;(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.	<ul style="list-style-type: none">In the Logical Interfaces box, select All Interfaces.To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, 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>.

PART 1

Overview

- [Logging and Reporting Overview on page 3](#)
- [Junos Space Security Director Logging and Reporting on page 7](#)
- [Junos Space Security Director Logging and Reporting on the JA2500 Appliance in an Integrated Environment on page 23](#)
- [Log Director on page 29](#)
- [Security Director and SRX Series Device Settings for Logging on page 37](#)
- [Back Up and Restore Log Collector Data on page 43](#)

CHAPTER 1

Logging and Reporting Overview

This chapter includes the following topics:

- [Understanding Junos Space Security Director Logging and Reporting on page 3](#)
- [Understanding Role-Based Access Control on page 5](#)

Understanding Junos Space Security Director Logging and Reporting

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

The Logging and Reporting module provides:

- Device health and events monitoring.
 - Visualization of security events resulting from complex and dynamic firewall policies using dashboard and event viewer.
 - Device health monitoring of CPU and memory.
 - Alert notification about specific events or upon attaining threshold limit.
- Scalable VM-based log collection and Log Collector management.
- The JA2500 appliance as a hardware Log Collector or Log Concentrator.

Logging

Logs, also called event logs, provide vital information for managing network security incident investigation and response.

Logging provides the following features:

- Receives events from SRX Series Services Gateway and application logs.
- Stores events for a defined period of time or a set volume of data.
- Parses and indexes logs to help speed up searching.
- Provides queries and helps in data analysis and historical events investigation.

The system collects the following key logs:

- **Firewall**—Captures events generated by one or more firewall rules to validate whether the rules configured are producing the desired impact on actual traffic.
- **IDP**—Captures events when the system is attacked. If the configuration is enabled, the log captures the volume of messages transferred to an application. **For example:** from an IP address, to an IP address, and so on. It also logs details of the traffic permitted and dropped according to the IDP rule set.
- **VPN**—Captures the status of the VPNs and enables VPN monitoring.
- **UTM**—Captures all UTM-related log messages. **For example:** Antivirus records virus incidents in Web, FTP, and e-mail traffic.
- **System**—Captures the control plane logs generated and stored on the local SRX Series Services Gateways.

Monitoring

Logs allow you to monitor devices for issues to ensure that all services are up and running, and to check on the device usage trends to allow you make decisions about potential issues and upgrades.

Security traffic monitoring helps to ensure that the security practices and controls are in place, are being adhered to, and are effective. You can view traffic logs generated from security policies, using the dashboard and event viewer.

Alert and Notifications

Alerts and notifications are used to notify administrators about significant events within the system. Notifications can also be sent through e-mail.

You will be notified when predefined network traffic condition. Alert trigger threshold is number of network traffic events crossing a pre-defined threshold within a period of time.

Reports

Reports are used to schedule reports daily, weekly, or monthly, and configure them to include multiple criteria. You can also personalize the reports by adding company logo, footer and so on. When the system generates a report, you and other designated recipients receive the report in PDF format through e-mail. Reports enable you to perform trend analysis of your network activities.

Related Documentation

- [Understanding Role-Based Access Control on page 5](#)
- [Understanding the Log Collector Deployment Modes on page 7](#)
- [Prerequisites for Installing Junos Space Security Director Logging and Reporting in a JA2500 Appliance on page 24](#)

Understanding Role-Based Access Control

Domain role-based access control (RBAC) can be used to control access to Logging and Reporting. You must have **Security Analyst** or **Security Architect** or have permissions equivalent to that role to access the dashboard, event viewer, and alerts. While creating or modifying an alert definition and reports, you can search e-mail addresses of other space users only if you have permission to view **User account > Role based access control**. To create, modify, edit, and delete monitors and for different filter permissions, select all the options under **Role > Workspace and Tasks: Event viewer**.



NOTE:

- The dashboard, event viewer, filters, alerts and reports will not be visible unless you select either a predefined or a user-defined role.
- Logging and Reporting module supports only one level in domain hierarchy, that is there can be only one level of child domain under the Global domain.

Logging and Reporting module displays logs generated from the devices. Hence, the logs displayed in the domain that the user has logged in will display logs of the devices as defined in Junos Space Security Director. Domain RBAC has the following impact on logging and reporting:

- If you have logged in to a domain, logs from Event Viewer and the logs from the child domain (if you choose to allow users of this domain to have read-only access to parent domain) are displayed. If you have logged in to the Global domain, logs that do not have domain information are also displayed.
- If you have logged in to a domain, aggregated views in the Event Viewer is based on the logs from the domain and the logs from all the children domains (if you choose to allow users of this domain to have read-only access to parent domain). If you have logged in to the Global domain, aggregated views displays logs that do not have domain information
- If you have logged in to a domain, event based monitors in dashboard displays logs from the domain and the logs from all the children domains (if you choose to allow users of this domain to have read-only access to parent domain) and logs that do not have domain information are also displayed.
- If you have logged in to a domain; when alerts are created or updated, alert criteria are applied to logs in the domain and the logs from all the children domains (if you choose to allow users of this domain to have read-only access to parent domain). If alerts are created before the flag is turned on, manually update the alert definitions for the logs from children domain to be considered for alert generation.

- If you have logged in to a domain, device and health monitors, you will be able to select devices from the domain and from all the children domain (if you choose to allow users of this domain to have read-only access to parent domain).
- If you have logged in to a domain, report is generated based on the domain based on the logs from the report definition domain and the logs from all the children domains (if you choose to allow users of this domain to have read-only access to parent domain).

To populate the logs with the correct domain and device information:

- Add all devices that send logs to the Junos Space Network Management Application Platform user interface.

**Related
Documentation**

- [Understanding Junos Space Security Director Logging and Reporting on page 3](#)
- [Understanding the Log Collector Deployment Modes on page 7](#)
- [Prerequisites for Installing Junos Space Security Director Logging and Reporting in a JA2500 Appliance on page 24](#)

CHAPTER 2

Junos Space Security Director Logging and Reporting

The chapter covers the following topics:

- [Understanding the Log Collector Deployment Modes on page 7](#)

Understanding the Log Collector Deployment Modes

- [Overview on page 7](#)
- [Specifications for Deploying a Log Collector Virtual Machine on an ESX Server on page 8](#)
- [Specifications for Deploying JA2500 as a Log Collector on page 9](#)
- [Prerequisites for Security Director Logging and Reporting on page 10](#)
- [Installing Junos Space Security Director on page 10](#)
- [Installing Virtual Log Collectors on page 11](#)
- [Installing a JA2500 Log Collector Appliance Image Using a USB Drive on page 11](#)
- [Deploying a Single Log Collector on page 15](#)
- [Deploying Multiple Log Collectors on page 17](#)
- [Adding the Log Collector Subsystem as a Specialized Node on page 21](#)
- [Upgrading the Log Collector on page 22](#)

Overview

You can deploy Log Collectors in a VM environment or using a JA2500 appliance. For easy scaling, begin with a single Log Collector and incrementally add dedicated Log Collectors, as your needs expand. You must configure a Log Concentrator if you are using more than one Log Collector.

In case of VM environment, a single OVA image is used to deploy a Log Collector and Log Concentrator. The image presents a configuration script after you log in. During setup, you can configure the node as either a Log Concentrator or a Log Collector. At deployment, the user must select appropriate memory and CPU configuration values, as appropriate for the role of the VM.

Beginning in Junos Space Security Director Release 14.1R2, you can deploy a JA2500 appliance as a Log Collector and a Log Concentrator. For a JA2500 appliance, you must install the ISO image. During the installation, you can configure the node type as a Log Collector or Log Concentrator. You can then add the node as a specialized node on Junos Space Network Management Platform.

You can use Log Collectors (VM/JA2500 appliance) in 2 different modes:

- Single Log Collector mode— For more information, see [“Deploying a Single Log Collector” on page 15](#).
- Multiple Log Collector mode— For more information, see [“Deploying Multiple Log Collectors” on page 17](#).

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

You can use [Table 3 on page 8](#) to decide if you require a single Log Collector or multiple Log Collectors.

[Table 3 on page 8](#) lists the required specifications for deploying a Log Collector VM on an ESX server for various sustained EPS rates. The EPS rates shown in [Table 3 on page 8](#) were achieved in a testing environment. Your results might differ, depending on your configuration and network environment.

Table 3: Specifications for Deploying a Log Collector/Log Concentrator VM on an ESX Server

Sustained EPS	Number of VMs	Log Collector			Log Concentrator		
		CPU	RAM	Disk Space	CPU	RAM	Disk Space
2,500	1 Log Collector	8 CPU Intel Xeon processor E5-2650 2GHz	16 GB	1 TB	NA	NA	NA
5,000	2 Log Collectors	2 CPU Intel Xeon processor E5-2650 2GHz	16 GB	1 TB	8 CPU Intel Xeon processor E5-2650 2GHz	16 GB	1 TB
	1 Log Concentrator						
7,500	3 Log Collectors	2 CPU Intel Xeon processor E5-2650 2GHz	16 GB	1 TB	8 CPU Intel Xeon processor E5-2650 2GHz	16 GB	1 TB
	1 Log Concentrator						
10,000	4 Log Collectors	2 CPU Intel Xeon processor E5-2650 2GHz	16 GB	1 TB	8 CPU Intel Xeon processor E5-2650 2GHz	16 GB	1 TB
	1 Log Concentrator						



NOTE: The default shipping configuration includes 500 GB of disk space, which can be increased to 1 TB disk storage space.

Table 4 on page 9 lists the supported version of VMware hypervisor.

Table 4: Supported Version of VMware Hypervisor

VMware Hypervisor	Hypervisor Version
VMware ESX	5.0 or later



NOTE: For Log Collector and Log Concentrator virtual machines, the CPU must be **SSSE3** instruction set compatible. If the CPU is not compatible with SSSE3, then creating alert rules causes log collection failure.

You might experience issues with throughput and latency with a disk speed of less than 80 Mbytes/s. Ensure that your appliance supports a minimum disk speed of 100 Mbytes/s.

The following command checks the disk speed for JA1500 and JA2500 appliances:



NOTE: Do not execute this command when the system is processing logs or using the disk resources.

```
time sh -c "dd if=/dev/zero of=ddfile bs=8k count=250000 && sync"
```

In the following example, the system reports a disk speed of 204 Mbytes/s.

Example:

```
[user@host ~]# dd if=/dev/zero of=./test bs=8k
^C153342+0 records in
153342+0 records out
1256177664 bytes (1.3 GB) copied, 6.14817 s, 204 MB/s
```

Specifications for Deploying JA2500 as a Log Collector

You can use Table 5 on page 9 to decide if you require a single Log Collector or multiple Log Collectors.

Table 3 on page 8 lists the sustained EPS rates for deploying JA2500 as a Log Collector and Log Concentrator. The EPS rates shown in Table 5 on page 9 were achieved in a testing environment. Your results might differ, depending on your configuration and network environment.

Table 5: Deploying JA2500 as a Log Collector/Log Concentrator

Sustained EPS	JA2500 Log Collector	JA2500 Log Concentrator
5,000	1 Log Collector	X
10,000	2 Log Collectors	1 Log Concentrator

Prerequisites for Security Director Logging and Reporting

To use the Junos Space Security Director Logging and Reporting module, your system must meet the following prerequisites:

- Beginning with Release 14.1R2, the Security Director, Log Director, and Security Director Logging and Reporting applications are installed using a single Security Director image. For example: **Security-Director.14.1R2.x.img**.
- You must deploy the Log Collector for receiving and viewing logs.
- The Junos Space Network Management Platform VM must be deployed on the ESX server.
- The Platform must be configured with Ethernet Interface eth0 and management IP addresses. Note that the platform can also run on a JA2500 appliance.
- The Junos Space Network Management Platform must be up and running, and you must be able to log in to the Junos Space Network Management Platform user interface.
- The following ports must be open between the space server and the Log Collector:
 - Port 8004—Used for communication between the space and the node agent.
 - Port 50102—Used for log data queries.
 - Port 50105—Used for configuring the Log Concentrator.
 - Port 50002—Used for communication between the Log Collector and Log Concentrator.

Installing Junos Space Security Director

To install the Junos Space Security Director:



.....

NOTE:

- Beginning with Junos Space Security Director Release 14.1R2, a single image installs Security Director, Log Director, and Security Director Logging and Reporting module. Installing Security Director Release 14.1R2, installs all the 3 applications.
-

1. Download the latest Junos Space Security Director from the download site. For example: **Security-Director.14.1R2.6.img**.
2. Install Junos Space Security Director.
3. After successful installation, log out and log in to the Junos Space Network Management Platform user interface.

To validate the installation, select Security Director from the drop-down and check if the dashboard, event viewer, reports and alerts nodes are displayed.



NOTE: The Security Director UI Nodes display data when Log Director is installed and the Log Collector virtual machine is added as a specialized node. If the Log Collectors are added and functioning properly, there will not be any error message. If not, there will be appropriate error messages shown on these nodes.

Installing Virtual Log Collectors

1. Download the **Log-Collector-ESX.14.1R2.X.ova** file from the [Download Site](#).
2. Install the OVA image to deploy a Log Collector or Log Concentrator on to ESX server.
3. Add the Log Collector subsystem as a specialized node on the Junos Space Network Management Platform Fabric. For more information, see “[Adding the Log Collector Subsystem as a Specialized Node](#)” on page 21 for instructions on adding the Log Collector nodes as a specialized node.



NOTE: The virtual logging nodes can be added to Junos Space Network Management Platform running on both virtual and JA2500 environment.

Installing a JA2500 Log Collector Appliance Image Using a USB Drive

This topic applies to JA2500 appliance:



NOTE: The JA2500 appliance is not preinstalled with Junos Space Network Management Platform, in contrast with Junos Space.

You can install a Log Collector JA2500 image on a JA2500 appliance using a standard USB drive; both USB 2.0 and USB 3.0 are supported. You can use this procedure to restore the factory settings on an appliance.

Before you begin, ensure that:

- You have a laptop or PC that is connected to the Internet.
- You have access to any third party conversion tool (for example, Rufus <https://rufus.akeo.ie/>) for making a USB installer from the ISO image.



NOTE: Disclaimer: Juniper does not endorse any particular conversion tool. Juniper disclaims any and all assurances, representations and warranties of any kind, express or implied, including without limitation any warranty as to quality, merchantability or non-infringement, as to any third party software tools. Your use of such software is entirely at your own risk.

- You have a USB drive with at least 4 GB of free space. If there is not enough space then the disk will be formatted and you lose all the data on the USB drive.
- You can connect to the appliance using the management console.
- You have configured a console terminal or terminal emulation utility to use the following serial connection parameters:
 - Baud rate: 9600 bits per second
 - Data: 8 bits
 - Flow control: None
 - Parity: None
 - Stop bits: 1



NOTE: The console terminal or terminal emulation utility maps every key on the keyboard to a code that it then sends through the management console. In some cases, the Delete key on a PC keyboard does not send a DEL or Control-? character. You must ensure that the terminal utility that you are using to connect to the appliance maps a key to the DEL or Control-? character. Typically, this is accomplished by configuring the terminal utility to send a DEL or Control-? character when the Backspace key on the keyboard is pressed.

This installation procedure has the following steps:

1. Creating a bootable USB drive.
2. Ensuring that the appliance's BIOS boots from the USB drive instead of the appliance's hard disk.
3. Installing the ISO image on the JA2500 appliance.
4. Selecting the node type as Log Collector or Log Concentrator while installing the ISO image.

To install a software image (*.iso) on a JA2500 appliance using a USB drive:

1. Plug the USB drive into the USB port of a laptop or PC that is connected to the Internet.
2. Using a Web browser, navigate to the Juniper Networks Junos Space Security Director software download site, <http://www.juniper.net/support/downloads/?p=spacesecdir#sw>, and click **Log Collector ISO Image for JA2500 Appliance** to download the Log Collector USB bootable image.

The filename of the downloaded image is **Log-Director-version.spin-number.iso**, where *version* refers to the major version number and *spin-number* refers to the spin number within that release; for example, **Log-Director-JA2500.14.1R2.X.iso**.

3. Create a bootable USB drive by using one of the following procedures:

**NOTE:**

- If the USB drive has files that you would like to keep, save the files to your PC or laptop before you begin this procedure.
- The bootable USB drive that you create using these procedures will not be usable as a normal USB drive. If you want to use the USB drive for storing files, you must reformat the drive.

- If you are using a computer with Windows as the operating system, do the following:
 - a. Open the Rufus software, which was installed on your computer.
 - b. In the Rufus window, click the Open or Browse icon. In the subsequent dialog box, select the image file that you want to copy to the USB drive.
 - c. In the Rufus window, verify that the drive letter displayed in the Device drop-down box matches the chosen USB drive. If a different drive letter is displayed, select the drive letter that matches the USB device from the Device list.
 - d. Click **Start** and, in the confirmation dialog box that appears, click **Yes**.

A progress bar on the Rufus window displays the status; if the write operation is successful, a message is displayed.

- e. Click **Exit** to exit the window.
 - f. Eject the USB drive, and unplug it from the computer.
- If you are using a computer with Linux as the operating system, do the following to create a bootable USB drive:
 - a. Use install-mbr, parted, mkfs.vfat, syslinux packages for making the USB drive bootable.
 - b. Use the **mount -r -o loop (logdirector.iso) /mnt/cdrom** command to mount the ISO file to /mnt/cdrom.
 - c. Type the following command to copy the image file to the USB drive, and press Enter.

```
usb=$1 # usb drive location, i.e. /dev/sdb
suffix=1
part=$usb$suffix # usb fat partition which will be created /dev/sdb1
echo Installing ISO on the usb $usb on part $part
echo "installing mbr" install-mbr $usb --force
echo "making partitions" parted -s $usb mklabel msdos
parted -s $usb mkpart primary fat32 0 100%
parted -s $usb set 1 boot on
echo "making filesystem"
mkfs.vfat -F 32 -n SYSRESC $part
mkdir /tmp/usbdribe
mount -t vfat $part /tmp/usbdribe
cp -r --remove-destination /mnt/cdrom/* /tmp/usbdribe/
mv /tmp/usbdribe/isolinux/isolinux.cfg /tmp/usbdribe/isolinux/syslinux.cfg
mv /tmp/usbdribe/isolinux /tmp/usbdribe/syslinux sed -i -e
's!/isolinux!/syslinux!/g' /tmp/usbdribe/syslinux/grub.conf
```

```
umount $part syslinux --install --directory syslinux $part sync
```

The image file is copied to the USB drive and you are taken to the command prompt.

d. Eject the USB drive and unplug it from the computer.

4. Plug the USB drive into the USB port of the JA2500 appliance on which you want to install the software image.



NOTE: To install the software image from the USB drive, the boot priority order in the appliance must have USB boot at the top. By default, the appliance attempts to boot from the USB drive first and then from the RAID volume or hard drive. However, if you have changed the boot order in the BIOS of the appliance, you must access the boot menu and change the boot order. You do this by sending the DEL or Control-? character three times as soon as you power on the appliance.

5. To access the appliance boot menu, do the following:

- a. Power on the appliance.
- b. As soon as the appliance starts powering on, press the key that you have mapped to send the DEL character in the terminal emulation utility. In most cases, this would be the Backspace key.



NOTE: If the hard disk LEDs begin to flash at this point for more than a few seconds, the appliance is booting from the hard disk instead of the USB drive, and the BIOS menu will not be loaded. In this case, you need to power down the appliance and repeat this step.

If you are successful in accessing the BIOS setup, the boot menu appears after about one minute.

6. 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, do the following:
 - Use the down arrow 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.
 - Press the F4 key to save your changes and exit the BIOS setup.
7. After you have confirmed the BIOS setting, power off the appliance.
8. Power on the appliance again. The boot prompt displays the following menu:

Install Log Collector on Juniper Hardware
Install Log Concentrator on Juniper Hardware
Boot from Local Drive

- Select **Install Log Collector on Juniper Hardware** to install JA2500 as a Log Collector.
- Select **Install Log Concentrator on Juniper Hardware** to install JA2500 as a Log Concentrator.

Press the Enter key at the boot prompt to install the image from the USB drive. After completing the installation, remove the USB drive from the device and then reboot the system.



NOTE: For the JA2500 appliance, the installation process takes approximately 30 minutes. When the installation is complete, the appliance powers down.

9. After the appliance has powered down, remove the USB drive from the appliance.



NOTE: Because the appliance boot order was changed earlier in this procedure, the appliance will try to boot from the USB drive before choosing the next option. If the USB was not removed after the installation and the appliance is powered back on, you can select Boot from Local Drive from the USB install menu as above. You can change the boot order of the appliance at any time using the method explained previously in this procedure.

After the installation you must configure the IP address, Time Zone, and NTP settings. See [“Configuring Multiple Log Collectors and a Log Concentrator” on page 19](#) for more information.

Deploying a Single Log Collector

This example shows how to deploy a single Log Collector. With one Log Collector, the system queries using the connected Log Collector.

- [Requirements on page 15](#)
- [Overview on page 15](#)
- [Configuration on page 16](#)

Requirements

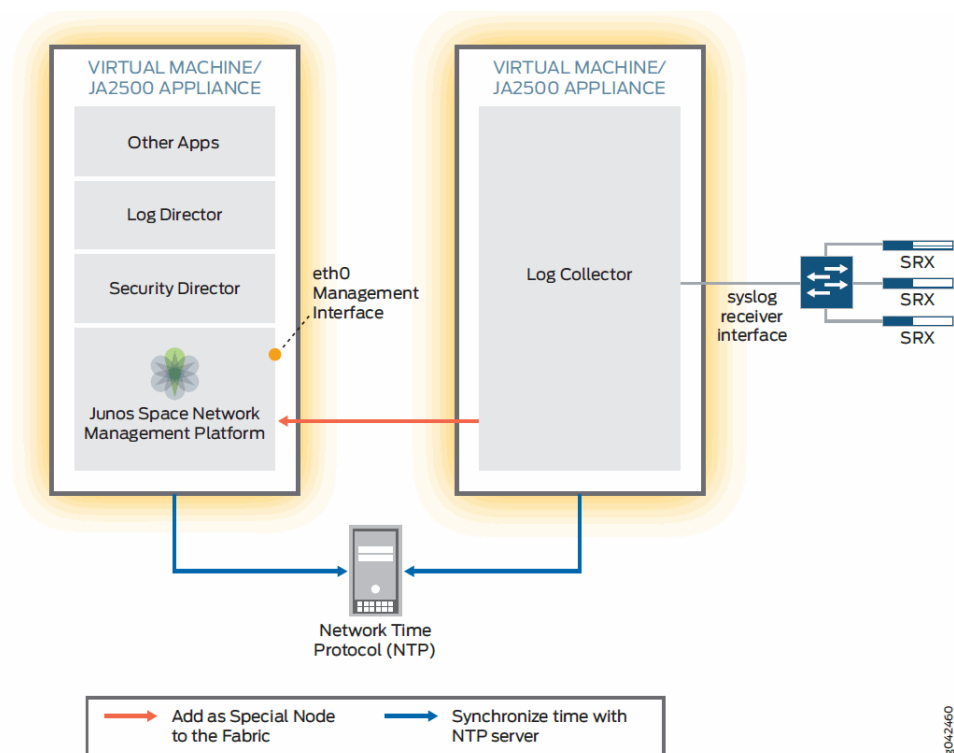
“Prerequisites for Security Director Logging and Reporting” on page 10 lists the prerequisites to use the Junos Space Security Director Logging and Reporting module.

Overview

Topology

[Figure 1 on page 16](#) shows a deployment example using a single Log Collector. This configuration provides an EPS rate of approximately 2,500.

Figure 1: Using a single Log Collector



8042460

Configuration

To configure a single Log Collector, perform these tasks:

- [Installation on page 16](#)
- [Configuring a Single Log Collector on page 16](#)
- [Adding the Log Collector Subsystem as a Specialized Node on page 16](#)

Installation

- Step-by-Step Procedure**
- For installing virtual Log Collector, see “Installing Virtual Log Collectors” on page 11.
 - For installing JA2500 appliance as a Log Collector, see “Installing a JA2500 Log Collector Appliance Image Using a USB Drive” on page 11.

Configuring a Single Log Collector

- Step-by-Step Procedure** See “Configuring Multiple Log Collectors and a Log Concentrator” on page 19 for the configuration procedure.

Adding the Log Collector Subsystem as a Specialized Node

- Step-by-Step Procedure** See “Adding the Log Collector Subsystem as a Specialized Node” on page 21 for the configuration procedure.

Deploying Multiple Log Collectors

If you have a scenario where you require more log reception capacity or events per second (EPS), you must add multiple Log Collectors.

Multiple Log Collectors require a Log Concentrator to aggregate the logs and to serve queries. Multiple Log Collectors provide higher rates of logging and better query performance. You can add up to four separate Log Collector VMs on the Junos Space Network Management Platform along with a Log Concentrator.

In case of VM environment, a single OVA image is used to deploy a Log Collector and Log Concentrator. The image presents a configuration script after you log in. During setup, you can configure the node as either a Log Concentrator or a Log Collector. At deployment, the user must select appropriate memory and CPU configuration values, as appropriate for the role of the VM.

For a JA2500 appliance, you must install the ISO image. During the installation, you can configure the node type as a Log Collector or Log Concentrator. You can then add the node as a specialized node on Junos Space Network Management Platform either as a Log Concentrator or as a Log Collector.

The use of multiple Log Collectors provides the following benefits:

- Improves performance.

For a VM-based Log Collector, you can achieve a sustained EPS rate of 2,500 per Log Collector.

For a JA2500 appliance-based Log Collector, you can achieve a sustained EPS rate of 5,000 per Log Collector.

- Provides high-volume log storage on a virtual device.
- Provides scalability for log collection and management.

It is important to consider different scenarios and system behavior while adding the specialized nodes to decide whether to deploy a single Log Collector or multiple Log Collectors.

- With one Log Collector, the system queries using the connected Log Collector.
- With multiple Log Collectors, the Log Concentrator aggregates the queries.

This example shows how to deploy multiple Log Collectors with a Log Concentrator.



NOTE: You cannot change the node type after you install the .iso image; you must reinstall the image.

- [Requirements on page 18](#)
- [Overview on page 18](#)
- [Configuration on page 19](#)

Requirements

“Prerequisites for Security Director Logging and Reporting” on page 10 lists the prerequisites to use the Junos Space Security Director Logging and Reporting module.

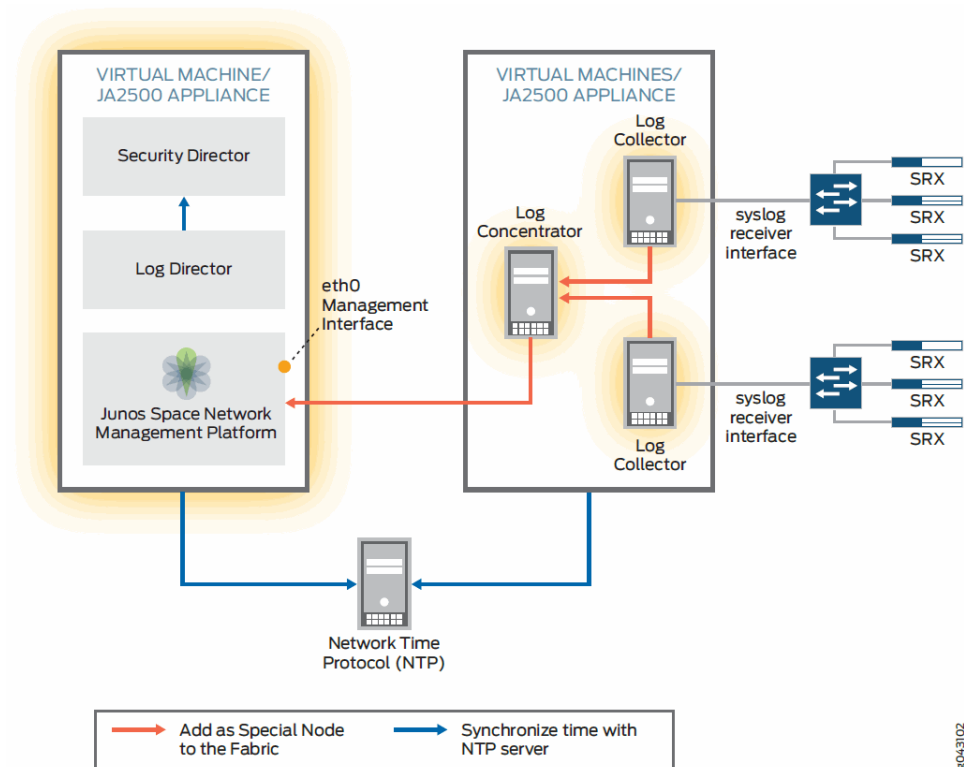
Overview

This example shows a deployment scenario of multiple Log Collectors along with a Log Concentrator. At deployment, the user must select appropriate memory and CPU configuration values, as appropriate for the role of the VM or appliance. For configuration values and EPS for VM and JA2500 appliance, see [Table 3 on page 8](#) and [Table 5 on page 9](#) respectively.

Topology

[Figure 2 on page 18](#) shows a deployment example using two Log Collectors. This configuration provides an EPS rate of approximately 5,000 for VM and 10,000 for JA2500 appliance.

Figure 2: Using multiple Log Collectors in a Virtual Environment or using JA2500 Appliance



NOTE: The Log Collector and the Log Concentrator must be added as a specialized node to the Junos Space Network Management Platform fabric.

Configuration

To configure multiple Log Collectors and a Log Concentrator, perform these tasks:

- [Installation on page 19](#)
- [Configuring Multiple Log Collectors and a Log Concentrator on page 19](#)

Installation

Step-by-Step Procedure

You must complete the following installation procedures before configuring the Log Collector.

- [“Installing Junos Space Security Director” on page 25.](#)
- For installing virtual Log Collector, see [“Installing Virtual Log Collectors” on page 11.](#)
For more information on deploying the Junos Space Network Management Platform virtual machine on the ESX server, see [Junos Space Network Management Platform.](#)
- For installing JA2500 appliance as a Log Collector, see [“Installing a JA2500 Log Collector Appliance Image Using a USB Drive” on page 11.](#)

Configuring Multiple Log Collectors and a Log Concentrator

Step-by-Step Procedure

To configure multiple Log Collectors, perform these tasks:

1. **Virtual Log Collectors:** Deploy the OVA image and configure it either as a Log Collector or a Log Concentrator. The image file can be downloaded from the download site. For example, LogCollector.14.1R2.12.ova.

You must deploy the OVA image multiple times depending on the number of Log Collectors. You must deploy a Log Concentrator for multiple Log Collectors.

JA2500 Log Collectors: Install the ISO image and configure it either as a Log Collector or Log Concentrator. For example, Log-Director-JA2500.14.1R2.x.iso. See [“Installing a JA2500 Log Collector Appliance Image Using a USB Drive” on page 11.](#)
2. Configure the VM/JA2500 appliance according to the requirement. See [Table 3 on page 8](#) and [Table 5 on page 9.](#)
3. Log in to the VM/JA2500 appliance using **root** as username and **juniper123** as the password.



NOTE: The Log Collector and the Junos Space Network Management Platform must be synchronized with the NTP server.

4. You will be prompted to change the root password.



NOTE: Use the changed password while adding the Log Collector or Log Concentrator as a specialized node in the Junos Space Network Management Platform.

5. For VM setup, you must configure the node type as a Log Collector or Log Concentrator using the following steps.

To configure the system as a Log Collector or a Log Concentrator, take either of these options.

- Enter your choice as **1** to configure the system as a Log Collector. When you are prompted to continue, enter **y**.
- Enter your choice as **2** to configure the system as a Log Concentrator.



NOTE: For JA2500 appliance setup, the Log Collector or Log Concentrator is configured during the installation procedure. See [Step 8 of “Installing a JA2500 Log Collector Appliance Image Using a USB Drive” on page 11.](#)

6. After selecting the node type, you will be prompted to configure the IP address, Time Zone, Name Server, and NTP Settings.

- 1) Configure IP Address
- 2) Configure Time Zone
- 3) Configure Name Server Settings
- 4) Configure NTP Settings
- 5) Quit

7. Type **1** to configure the IP Address and press Enter.

You are prompted to configure the IP address for the eth0 and eth1 interfaces.

- a.
 - 1) Configure eth0 IP Address
 - 2) Configure eth1 IP Address
- b. Type **1** to configure the eth0 IP address. Type the IP address for the eth0 interface in dotted decimal notation and press Enter. Enter the subnet mask and then the default gateway.
- c. Type **2** to configure the eth1 IP address. Type the IP address for the eth1 interface in dotted decimal notation and press Enter. Enter the subnet mask and then the default gateway.

8. Type **2** to configure the time zone and press Enter.

You are prompted to identify a location so that the time zone rules can be set correctly.

- a. For example:

Please select a continent or ocean.

- 1) Africa
- 2) America
- 3) Antartica
- 4) Arctic Ocean
- 5) Asia

Please select a country.

- 1) Africa
 - 2) America
 - 3) Antartica
 - 4) Arctic Ocean
 - 5) Asia
- b. Enter the location and confirm the changes.
9. Type **3** to configure the Name Server settings, and press Enter.
- You are prompted to enter the Name Server IP address.
- Enter the Name Server IP address**
10. Type **4** to configure the NTP settings, and press Enter.
- You are prompted to enter the NTP server IP address or domain name.
- a. **Enter NTP server IP address or domain name.**
11. Type **5** to quit.
12. Add multiple Log Collectors or a Log Concentrator as a specialized node on the Junos Space Network Management Platform Fabric. For more information, see [“Adding the Log Collector Subsystem as a Specialized Node” on page 21](#).
13. Configure the parameters and the Global settings for Log Collector. For more information, see [Table 9 on page 31](#) and [Table 12 on page 35](#).

Adding the Log Collector Subsystem as a Specialized Node

To add the Log Collector subsystem as a specialized node on the Junos Space Network Management Platform:

1. Navigate to **Network Management Platform > Administration > Fabric > Add Fabric Node**. The Add Node to Fabric dialog box is displayed.
2. In the dialog box, enter a name for the node and the IP address of the Log Collector subsystem.
3. Click **Add as a specialized node**.
 - In the User field, enter the username as **root**.
 - In the Password field, enter the root password that you changed while deploying the Log Collector.
4. Click **Add** to add the node to the fabric.

To validate the installation,

1. To view the newly added node:

Select **Network Management Platform > Administration > Fabric**.
2. To check if the dashboard, event viewer and alerts nodes are displayed.

Select **Network Management Platform > Administration > Logging > Log Collectors**.

Upgrading the Log Collector

You can upgrade the Log Collector nodes by installing the Log Collector upgrade package. The procedure is the same for both the virtual and hardware space environments. The support for hardware-based Log Collectors is available from Release 14.1R2. You must upgrade log collection on VM nodes and hardware-based nodes (JA2500) by following the steps as listed below.

Note that all the nodes that are present in the system will be upgraded with this upgrade package.

To upgrade Log Collector, perform the following steps:

1. Take a backup of log data from the Log Collector. For more information, see [“Backing Up Log Collector Data” on page 44](#) for instructions on backing up the data for Log Collector.
2. Download the **Log-Collector-Upgrade.14.1R2.3.img** file from the [Download Site](#).
3. Select **Network Management Platform > Administration > Applications** and then click the **Add Application** icon.

Upload the image using the **Upload via HTTP** or **Upload via SCP** option.

4. Select Log Collector. For example: **Log-Collector-Upgrade.14.1R2.3.img**. The option to install is displayed.
5. Click the Add Application icon to install the Log Collector upgrade application.
6. Select the Log Collector upgrade and then click **Install**.

The Job Management tab shows the image upgrade status. To validate the upgrade status of Log Collector nodes, select **Logging > Log Collectors > Version**.



NOTE:

- During the Log Collector node upgrade the node goes down during which the logs will not be received.
 - A post upgrade consistency check is performed based on the volume of data collected. The actual time for the consistency check depends on the data inconsistency (if any) and the volume of data already collected. Note that the Log Collector does not receive any logs during the consistency check.
 - If the upgrade fails on any of the nodes, you must the reinstall the upgrade image.
 - If you are using multiple Log Collectors and have changed your Log Collector Password (using “Change Password” in Log Collectors page) in Release 14.1R1, then you have to “reset the password” after the upgrade of Log Collectors to Release 14.1R2 .
-

CHAPTER 3

Junos Space Security Director Logging and Reporting on the JA2500 Appliance in an Integrated Environment

In this section, the JA2500 as an integrated deployment runs Junos Space, Security Director, Log Director, and Log Collector VM. .

This chapter includes the following topics:

- [Installation Steps Overview on page 23](#)
- [Prerequisites for Installing Junos Space Security Director Logging and Reporting in a JA2500 Appliance on page 24](#)
- [Specifications for Log Collector VM Installation on a JA2500 Appliance on page 25](#)
- [Installing Junos Space Security Director on page 25](#)
- [Installing the Log Collector VM Application on the Junos Space Network Management Platform on page 26](#)
- [Adding the Log Collector Subsystem as a Specialized Node on page 28](#)

Installation Steps Overview

This deployment involves the following steps:

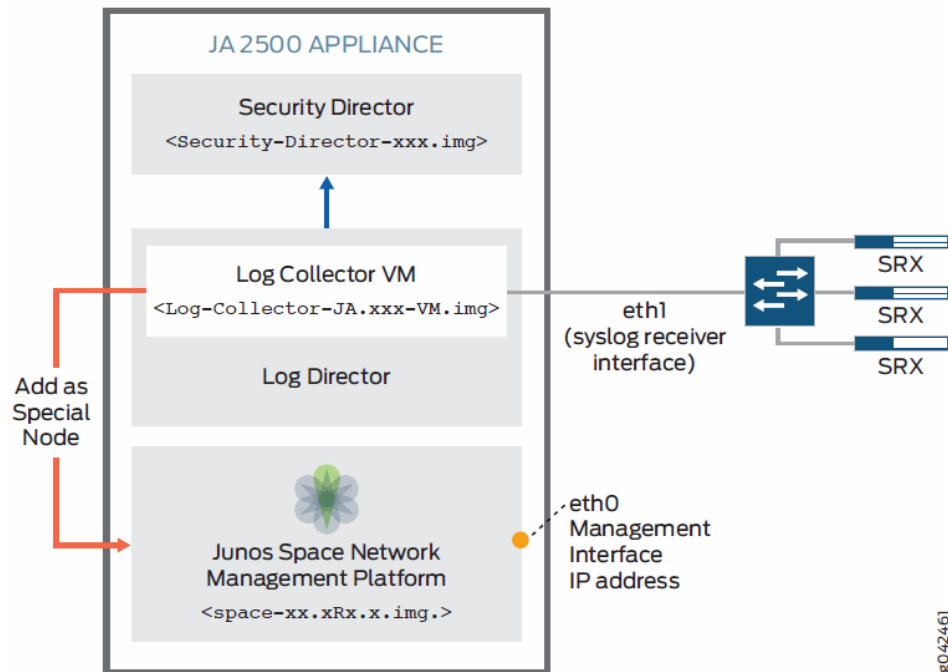
- Installing Junos Space Network Management Platform on a JA2500 appliance. For more information see, [Junos Space Network Management Platform](#)
- Installing Junos Space Security Director on page 25
- Installing the Log Collector VM Application on the Junos Space Network Management Platform on page 26
- Adding the Log Collector Subsystem as a Specialized Node on page 28



NOTE: Add the Log Collector Virtual Machine as a specialized node after installing Log Collector VM application.

Figure 3 on page 24 shows the setup for Junos Space Security Director Logging and Reporting in JA2500 appliance.

Figure 3: Junos Space Security Director Logging and Reporting in JA2500 Appliance Setup



Prerequisites for Installing Junos Space Security Director Logging and Reporting in a JA2500 Appliance

Prerequisites are:

- Junos Space Network Management Platform 14.1R2.9 must be installed on a JA2500 appliance from the download site. Example: **space-14.1Rx.x.img**.
- The following ports must be open between eth0 and eth1 on the device:
 - Port 8004—Used for communication between the space and the node agent
 - Port 50102—Used for log data queries
- The Junos Space Network Management Platform must be configured with Ethernet Interface eth0 and Management IP addresses.
- Ethernet Interface eth1 must be connected to the network to receive logs.
- The Junos Space Network Management Platform must be up and running and you must be able to log in to the Junos Space Network Management Platform user interface.



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

- Related Documentation**
- [Understanding Junos Space Security Director Logging and Reporting on page 3](#)
 - [Installation Steps Overview on page 23](#)
 - [Specifications for Log Collector VM Installation on a JA2500 Appliance on page 25](#)
 - [Understanding How Junos Space Uses Ethernet Interfaces eth0 and eth3](#)

Specifications for Log Collector VM Installation on a JA2500 Appliance

Table 6 on page 25 lists the required specifications for installing the Log Collector VM application on a JA2500 appliance.



NOTE: These specifications will be internally used from the JA2500 by the Log Collector subsystem.

Table 6: Specifications Required to Install the Log Collector Subsystem on a JA2500 Appliance

Component	Specification
Memory	8 GB
Disk space	600 GB
CPU	2 CPUs of 3.20 GHz

- Related Documentation**
- [Installation Steps Overview on page 23](#)
 - [Prerequisites for Installing Junos Space Security Director Logging and Reporting in a JA2500 Appliance on page 24](#)
 - [Installing the Log Collector VM Application on the Junos Space Network Management Platform on page 26](#)

Installing Junos Space Security Director

To install the Junos Space Security Director:



NOTE:

- Beginning with Junos Space Security Director Release 14.1R2, a single image installs Security Director, Log Director, and Security Director Logging and Reporting module. Installing Security Director Release 14.1R2, installs all the 3 applications.

1. Download the latest Junos Space Security Director from the download site. For example: **Security-Director.14.1R2.6.img**.

2. Install Junos Space Security Director.
3. After successful installation, log out and log in to the Junos Space Network Management Platform user interface.

To validate the installation, select Security Director from the drop-down and check if the dashboard, event viewer, reports and alerts nodes are displayed.



NOTE: The Security Director UI Nodes display data when Log Director is installed and the Log Collector virtual machine is added as a specialized node. If the Log Collectors are added and functioning properly, there will not be any error message. If not, there will be appropriate error messages shown on these nodes.

- Related Documentation**
- [Understanding Junos Space Security Director Logging and Reporting on page 3](#)
 - [Understanding Role-Based Access Control on page 5](#)

Installing the Log Collector VM Application on the Junos Space Network Management Platform

To install the Log Collector VM application on the Junos Space Network Management Platform:

1. Log in to the Junos Space Network Management Platform user interface.
The box at the top of the task tree displays Junos Space Network Management Platform by default.
2. Select **Network Management Platform > Administration > Applications**.
3. Click the **Add Application** icon.
4. Upload the Log Collector VM image (Log-Collector-JA.14.1R2.X-VM.img) by performing either of the following steps:
 - a. Click **Upload via SCP**.

The Upload Software via SCP dialog box appears. You must provide the following Secure Copy remote machine credentials:

- Add your username.
- Add your password.
- Confirm by adding your password again.
- Add the host IP address.

- Add the local pathname of the Junos software application file.
 - Click **Upload**.
5. To verify that the Upload Application job is complete, click **Job ID** on the Jobs > Job Management inventory page. Wait until the job is completed and to ensure that the job is successful.



NOTE: If the upload is successful, Log Collector VM is displayed on the Add Application page. The details of the application title, filename, version, release type, and the required Junos Space Network Management Platform version are also displayed.

6. Click the Add Application icon to install the Log Collector VM application.
7. Select the Log Collector VM image.
8. Click **Install**.

The Application Configuration dialog box is displayed.

9. Enter the IP address, subnet mask, default gateway, and the password for the Log Collector VM application. You are also prompted to configure the IP address for eth1 and eth2 interfaces.



NOTE: You will be prompted twice to enter the password. Use this password while adding a Log Collector virtual machine as a specialized node in the Junos Space Fabric.

10. Click **OK** to proceed.

The Application Management Job Information dialog box appears.

11. In the Application Management Job Information dialog box, click **Job ID** to see the Add Application job on the Jobs > Job Management inventory page. Wait until Log Director is fully deployed to ensure that the job is successful.
12. Log out from and log in to the Junos Space Network Management Platform for the changes to take effect.



NOTE: Ensure that you can ping the Log Collector subsystem using the configured IP address.

Related Documentation

- [Installation Steps Overview on page 23](#)
- [Prerequisites for Installing Junos Space Security Director Logging and Reporting in a JA2500 Appliance on page 24](#)
- [Specifications for Log Collector VM Installation on a JA2500 Appliance on page 25](#)
- [Adding the Log Collector Subsystem as a Specialized Node on page 28](#)

Adding the Log Collector Subsystem as a Specialized Node

To add the Log Collector subsystem as a specialized node on the Junos Space Network Management Platform:

1. Navigate to **Network Management Platform > Administration > Fabric > Add Fabric Node**. The Add Node to Fabric dialog box is displayed.
2. In the dialog box, enter a name for the node and the IP address of the Log Collector subsystem.
3. Click **Add as a specialized node**.
 - In the User field, enter the username as **root**.
 - In the Password field, enter the root password that you entered in step 9 of [“Installing the Log Collector VM Application on the Junos Space Network Management Platform”](#) on page 26.
4. Click **Add** to add the node to the fabric.

The node **Logging** appears under **Administration > Logging**.

The Log Collector subsystem IP address is displayed under **Administration > Logging > Log Collector**.

Log Director is now ready to receive logs.

Related Documentation

- [Installation Steps Overview on page 23](#)
- [Prerequisites for Installing Junos Space Security Director Logging and Reporting in a JA2500 Appliance on page 24](#)
- [Specifications for Log Collector VM Installation on a JA2500 Appliance on page 25](#)
- [Adding a Node to the Fabric](#)

CHAPTER 4

Log Director

The chapter covers the following topics:

- [Log Director Overview on page 29](#)
- [Logging on page 29](#)
- [Using Log Messages for Troubleshooting Issues on page 30](#)
- [Log Collectors on page 31](#)
- [Reporting Devices on page 33](#)
- [Global Settings on page 34](#)

Log Director Overview

Log Director is a plug-in on the Junos Space Network Management Platform, which is used for system log data collection for SRX Series devices running Junos OS. Log Director consists of two components: the Junos Space plug-in application, and a virtual machine (VM) deployment of Log Collectors and a Log Concentrator.

The Log Collector runs both on JA2500 and on a VM, which provides 500 GB of space for log storage. When the allocation threshold is exceeded, the oldest log file in the directory is deleted to make room for new system logging messages. To permanently store system logging messages, you must archive them to an external device. For more information on how to store to an external device, see [Table 9 on page 31](#).

Related Documentation

- [Log Collectors on page 31](#)
- [Reporting Devices on page 33](#)
- [Global Settings on page 34](#)

Logging

The Junos Space application includes a new node, which you can access from the left navigation pane of Junos Space Network Management Platform under **Administration > Logging**. You can use this node to manage, license, and configure the Log Collector for system log forwarding and backup.

Click **Network Management Platform > Administration > Logging > Reporting Devices** to view logging details.



NOTE: The Logging page allows you to view the current status of the license for Log Collector. The system validates the license expiration date and displays a warning message for an upcoming license expiration.

For example: The license of the Log Collector will expire in 30 days; please upgrade Log Director for uninterrupted use of the system.

Table 7 on page 30 provides the details of the logging parameters.

Table 7: Logging Parameters

Parameters	Details
License	
EPS License Limit	Specifies the average EPS per day. The default value is 500 EPS. You can enter the EPS value based on your license limit.
Previous Day's Stats	
Total Log Count	Specifies the total logs received on the previous day.
Average EPS	Specifies the average EPS received on the previous day.
Average Overall EPS	Specifies the graph of the average overall EPS across 90 days. A notification message is displayed if the user exceeds the licensed limit.

- Related Documentation**
- [Reporting Devices on page 33](#)
 - [Global Settings on page 34](#)
 - [Log Collectors on page 31](#)

Using Log Messages for Troubleshooting Issues

Log messages help you troubleshoot an issue by providing details about the issue.

Table 8 on page 30 provides the list of log messages.

Table 8: Log Messages

Log Message	Explanation	Corrective Action
Error while retrieving data. Log Collector may not be configured or accessible at this time. Please try again later	This message appears if the Log Collector is not configured properly or if it is not accessible.	Add a Log Collector as a specialized node through Network Management Platform > Administration > Fabric or check whether the status of Log Collector is up/down in Administration > Logging > Log Collectors page.

Table 8: Log Messages (*continued*)

Found multiple log decoders. Please add a concentrator or keep only one decoder for log director to work.	This message appears if the Log Concentrator is not configured for multiple Log Collectors.	Add a Log Concentrator as a specialized node through Network Management Platform > Administration > Fabric.
Couldn't find any decoders. Please add at least one decoder for log director to work.	This message appears if the Log Collector is not added.	Add a Log Collector as a specialized node through Network Management Platform > Administration > Fabric.
Active Log Collector not found.	This message appears if the Log Collector is not supported.	Verify if there is only one Log Collector or multiple Log Collectors. You must add a Log Concentrator if there are multiple Log Collectors.

- Related Documentation**
- [Log Director Overview on page 29](#)
 - [Reporting Devices on page 33](#)
 - [Global Settings on page 34](#)

Log Collectors

The Log Collector page provides you the options for viewing the Log Collector IP address and available free space, status, syslog forwarding, NFS mount storage, and export storage.

You can also change the database password from this page. If a new node is added, the password change is applicable on all nodes on the system for multiple Log Collectors.

Click **Network Management Platform > Administration > Logging > Log Collectors** to view details from the Log Collector page.

Log Collector nodes, name, IP, type Log Collector or Log Concentrator, Disk free space, version and the current setting status of the node.

[Table 9 on page 31](#) provides the details of the Log Collector parameters.

Table 9: Log Collector Parameters

Parameters	Details
General	
Name	Specifies the name of the Log Collector or a Log Concentrator.
IP	Specifies the IP address of the Log Collector or a Log Concentrator.
Type	Specifies the type of device. For example, Log Collector or Log Concentrator.

Table 9: Log Collector Parameters (*continued*)

Parameters	Details
Status	Specifies the current status of the Log Collector or Log Concentrator.
Disk Free Log Space	Specifies the free space in the Log Collector.
Version	Specifies the version of the Log Director.
License Expiry Date	Specifies the license expiration date of Log Director.
Settings	Specifies the settings that are enabled for the logging nodes.
NFS Mount Storage	
Enable NFS Mount Storage	Select this option to enable NFS storage instead of local system storage. If NFS mount storage is enabled, local system storage is not used to store logs and related data. We recommend not to share the same NFS mount points with multiple systems (Log Collectors).
Export Storage	
Enable Export Storage	Select this option to enable or disable export storage. This option allows you to export the local system storage to an NFS storage on a different server.
Syslog Forwarding	
NOTE: This is not applicable if the node is configured as a Log Concentrator.	Allows you to enable syslog forwarding. Selecting the check box displays the following options:
Enable Syslog Forwarding	<ul style="list-style-type: none"> IP Address—Specifies the IP address to which the syslog is forwarded. Port Number—Specifies the port number to which the syslog is forwarded. Protocol—Specifies the protocol to which the syslog is forwarded. The available protocols are TCP and UDP. Category—Specifies the filter options.

Log collection statistics is used to troubleshoot the issues with Log Collector or Log Concentrator. If you are not able to view any logs in the Event Viewer or dashboard, select **Action > Show statistics** to view more information or for troubleshooting issues with Log Collector.

Table 10 on page 32 provides the details and statistics of log collection.

Table 10: Log Collection Statistics

Collection Statistics	Description
Node name	Displays the name of the node.

Table 10: Log Collection Statistics (*continued*)

Management IP (IPv4)	Displays the IP address of the node.
Device type	Displays the type of the node. The node type can be a Log Collector or Log Concentrator.
First packet received	Displays the first log database entry time and date.
Last log received	Displays the last log database entry time and date.
Packets not processed	Displays the number of the packets that are not processed.
Forwarded log count	Displays the number of logs that are forwarded.
Current log rate	Displays the current log rate.
Maximum receive rate	Displays the maximum receive rate.
Total number of logs	Displays the total number of logs received by the Log Collector.

- Related Documentation**
- [Log Director Overview on page 29](#)
 - [Reporting Devices on page 33](#)
 - [Global Settings on page 34](#)

Reporting Devices

From the Reporting Devices page, you can aggregate logs based on device name, product family, and log servers.

Click **Network Management Platform > Administration > Logging > Reporting Devices** to view device options.

[Table 11 on page 33](#) provides the details of the settings parameters on the Reporting Devices page.

Table 11: Reporting Devices

Parameters	Details
Next Update	Specifies the time when the next update is executed. The information is updated at an interval of 24 hours.
Report Device Table	
Show	Specifies the devices that send logs. You can select All Devices or a specific device to display report device details.
Aggregate	

Table 11: Reporting Devices (*continued*)


Parameters	Details
Device Name	<p>Specifies the details of the device. The default details displayed are:</p> <ul style="list-style-type: none"> • Device Name—Specifies the name of the device. • Device IP—Specifies the IP address of the device. • Product Family—Specifies the product family. • Syslog Server IP—Specifies the IP address of the syslog server. • Log Count (Last 24 hours)—Specifies the log count for 24 hours.
Product Family	<p>Specifies the details of the product family. The default details displayed are:</p> <ul style="list-style-type: none"> • Product Family—Specifies the product family. • Log Count (Last 24 hours)—Specifies the log count for 24 hours.
Log Server	<p>Specifies the details of the log server. You can determine the load on multiple log servers and take appropriate action based on these details.</p> <ul style="list-style-type: none"> • Syslog Server IP—Specifies the IP address of the syslog server. • Log Count (Last 24 hours)—Specifies the log count for 24 hours aggregated on log server.
Top Events Reporting Device Chart	Displays the chart of the reporting devices for top events.

- Related Documentation**
- [Log Director Overview on page 29](#)
 - [Global Settings on page 34](#)
 - [Log Collectors on page 31](#)

Global Settings

Using Log Collector Global settings, you can change the log database password, enable data compression, and retention logs. Click **Network Management Platform > Administration > Logging > Global Settings** to view the Log Collector settings. [Table 12 on page 35](#) provides the details of the settings parameters.

Table 12: Global Log Collector Settings

Parameters	Details
Log Database Password	<p>Allows you to change the password. Click Change Password to change the existing password.</p> <p>If a new node is added, the password change applies to all the nodes on the system for multiple Log Collectors.</p>
Data Compression	
Enable Data Compression	Select this option to enable or disable data compression. This option is enabled by default.
Retention Period	
Enable Retention Period	<p>Allows you to enable retention period.</p> <p>Selecting the check box displays the following options:</p> <ul style="list-style-type: none">Retention Period—Specify the number of days the logs can be retained. <p>NOTE: Retention is applicable only if you have sufficient disk space to store data. Otherwise, the older logs will be rolled over irrespective of the retention period setting.</p>
<div> NOTE: Do not delete the system jobs that are automatically scheduled from the Job Management page. If you delete these jobs, the alerts are not sent to Log Director.</div>	

- Related Documentation
- Log Director Overview on page 29
 - Log Collectors on page 31
 - Reporting Devices on page 33

CHAPTER 5

Security Director and SRX Series Device Settings for Logging

The chapter covers the following topic:

- [Configuring Security Director and SRX Series Devices to Receive Logs on page 37](#)

Configuring Security Director and SRX Series Devices to Receive Logs

To configure syslog to receive SRX Series device logs, use one of these options:

- Select **Network Management Platform > Devices > Device Management**.

The Device Management page appears.

- Select **Security Director > Devices > Device Management**.

The Device Management page appears.

Configuring Security Logging

To configure security logging:

1. Right-click a device and select **Device Configuration > Modify Configuration**.

The View/Edit Configuration page appears.

2. Under the Security section, click **Security Logging**.

The Create Security Logging page appears, as shown in [Figure 4 on page 38](#).

Figure 4: Device Configuration—Create Security Logging Page

Create Security Logging

General Settings

Mode:

Source Address:

Format:

Rate-Cap: logs/second

Disable Logging: ☐

UTC-Timestamp: ☐

Event-rate: logs/second

Stream

Name	Host	Port	Severity	Category	Format

File

File Name:

File Path:

File Size: megabytes

Max No. Of files:

Cache

Ok Cancel

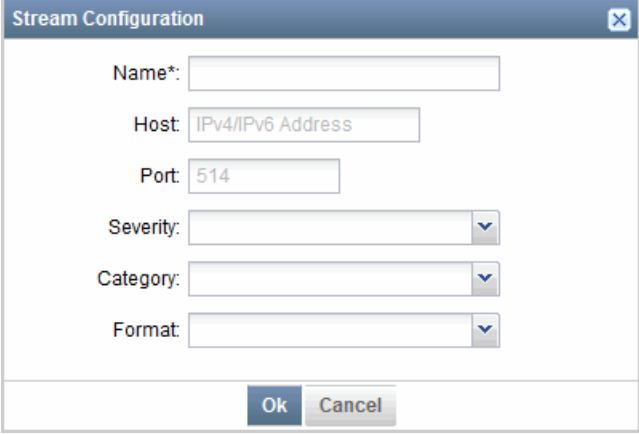
3. Under the General Settings section, configure the following parameters:
 - Mode—Select the mode of logging as **stream** or **event**.
 - Source Address—Enter the source IP address to be used to send logs.
 - Format—Select the logging format as **sd-syslog**.
 - Disable Logging—select the check box to disable security logging for a device.
 - UTC-Timestamp— (Optional) To use Coordinated Universal Time (UTC) for security log timestamps, select the check box.
 - Event-rate— (Optional) Enter the event rate to limit the rate per second at which logs are streamed.
4. Under the Stream section, configure the following parameters:

To create a new stream configuration:

- Click the plus sign (+).

The Stream Configuration page appears, as shown in [Figure 5 on page 39](#).

Figure 5: Security Logging—Stream Configuration Page



The image shows a 'Stream Configuration' dialog box with the following fields and controls:

- Name*:** A text input field.
- Host:** A text input field with a placeholder 'IPv4/IPv6 Address'.
- Port:** A text input field with the value '514'.
- Severity:** A dropdown menu.
- Category:** A dropdown menu.
- Format:** A dropdown menu.
- Buttons:** 'Ok' and 'Cancel' buttons at the bottom.

- Name—Enter the name of the new stream configuration.
- Host—Enter the IPv4 or IPv6 address of the Log Collector.



NOTE: You must configure the SRX Series device to send logs to a specific Log Collector. If you are using multiple Log Collectors, ensure that the load is balanced evenly across the Log Collectors.

- Port—Enter the port number.
- Severity—Select one of the following available required severity types:
 - Emergency
 - Alert
 - Critical
 - Error
 - Warning
 - Notice
 - Info
 - Debug
- Category—Select the type of category as **all** or **content-security**.
- Format—Select the type of format as **sd-syslog**.
- Click **Ok**.

You can modify or delete the existing streams. To modify or edit a stream, select the stream and click the pencil icon. To delete a stream, select the stream and click the minus sign (-).

5. To create a new security log, click **Ok**.

Modifying Syslog

To modify syslog:

1. Under the Security section, click **Syslog**.

The Modify Syslog page appears, as shown in [Figure 6 on page 40](#).

Figure 6: Device Configuration—Modify Syslog Page

2. In the General Settings section, configure the following parameters:
 - Time-format—Clear the check box to include additional information in the system log timestamp.
 - Source Address—Specify the source address for log messages.
 - Log-Rotate-Frequency—Specify the interval for checking log file size and archiving messages.



NOTE: Log-Rotate-Frequency field is applicable only when the configuration is for file.

- Allow duplicates—Select the check box to allow repeated messages in the system log output files.
3. You can send system logging information to one or more destinations. To send a security log to a remote server:

Under the Host section, configure the following parameters:

- To create a new host, click the plus sign (+).

The Host Configuration page appears, as shown in [Figure 7 on page 41](#).

Figure 7: Modify Syslog–Host Configuration Page

The screenshot shows the 'Host Configuration' dialog box. It has a title bar with 'Host Configuration' and a close button. The main area is divided into sections. The 'Name*' section has a dropdown menu with 'Type or select'. The 'Match' section is a large empty text area. The 'Contents' section has a table with two columns: 'Facility' and 'Severity'. Above the table are icons for adding, editing, and deleting. The 'Advanced Options' section has checkboxes for 'Allow duplicates' and 'Explicit priority', a 'Facility override' dropdown, and a 'Log prefix' text field. At the bottom are 'Ok' and 'Cancel' buttons.

- Name—Select the host name to notify.

You must set the hostname on the SRX Series device to receive syslog messages from Log Director.

To set the hostname:

set system host-name <srx-host>



NOTE: If the hostname is not configured on the SRX Series device, the Log Collector will not receive logs from the SRX Series device, and therefore the logs will not be displayed in the Event Viewer or on the dashboard.

- Under the Contents section, to configure the logging of system messages to the system console:
 - Click the plus sign (+), and the Contents page appears.
 - Facility—Select the class of messages to log.

- Severity—Select the message severity. Messages with severities of the specified level and higher are logged.
- Click **Ok**.
- Allow-duplicates—Select the check box to allow the repeated messages in the system log output files.
- Explicit priority—Select the check box to include the priority and facility in messages.
- Facility override—Select the alternate facility to select an alternate facility to substitute for the default facilities.
- Log prefix—Specify a text string to include in each message directed to a remote destination.
- Match—Specify a text string that must appear in a message for the message to be logged to a destination.
- Port—Enter the port number.
- Source Address—Specify the source address for log messages.
- Structured data—Select the check box to write system log messages to the log file in structured-data format.
- Click **OK**.

Enabling Logging on Branch SRX Series Devices

For more information about enabling logging on branch SRX Series devices, see [Enable Logging on Branch SRX Series Devices](#).

Enabling Logging on High-End SRX Series Devices

For more information about enabling logging on high-end SRX Series devices, see [Enable Logging on High End SRX Series Devices](#).

Related Documentation

- [Log Director Overview on page 29](#)
- [Understanding Role-Based Access Control on page 5](#)

CHAPTER 6

Back Up and Restore Log Collector Data

The procedures are the same for virtual environments and for JA2500 appliances.

If the logs are restored on the same Log Collector virtual machine (VM) that receives logs, Log Collector will not receive logs while data is being restored. For uninterrupted log collection, we recommend that you receive logs and restore data on different VMs.

The chapter covers the following topics:

- [Log Collector Database Files Overview on page 43](#)
- [Backing Up Log Collector Data on page 44](#)
- [Restoring Log Collector Data on page 45](#)

Log Collector Database Files Overview

Logs are parsed and stored as raw logs using key-value pair format at the location `/var/netwitness/logdecoder/`. [Table 13 on page 43](#) provides details about the log folders.

Table 13: Log Folder Details

Folder Name	Description	Database Files
Packetdb	Contains files that represent raw logs	<code>packet-000000001.nwpdb</code> <code>packet-000000002.nwpdb</code> <code>packet-000000003.nwpdb</code>
Metadb	Contains files with metadata information about the parsed fields	<code>meta-000000001.nwmdb</code> <code>meta-000000002.nwmdb</code> <code>meta-000000003.nwmdb</code>
Sessiondb	Contains files with session data corresponding to each log received	<code>session-000000001.nwsdb</code> <code>session-000000002.nwsdb</code> <code>session-000000003.nwsdb</code>

The database files are named in increasing numerical order. For instance, **packet-0000000002.nwpdb** follows **packet-0000000001.nwpdb**. The number of files and the numbering need not be the same across directories. Log files are not named according to their creation date; for this reason, a single file can contain data for more than one day, and a single day can have more than one log file associated with it.

- Related Documentation**
- [Backing Up Log Collector Data on page 44](#)
 - [Restoring Log Collector Data on page 45](#)

Backing Up Log Collector Data

Backing up Log Collector data involves copying files from the **logdecoder** directory folders and moving the files to another remote location. You should back up all the database files periodically, manually or by scheduling an automatic daily backup.

To back up Log Collector data:

1. Log in to the Log Collector VM as **root ssh root@Log-Collector-VM-IP**.
2. Navigate to the folder **cd /var/netwitness/logdecoder** and to the following folders:
 - **Packetdb**
 - **Metadb**
 - **Sessiondb**
3. Identify the files to be backed up in each directory:
 - Use file timestamp to group files for periodic backup.
 - Look for files up to the $(n-1)$ th file to be backed up. The n th file will be available for writing.
4. With SCP, copy files from the respective folders to a remote location using the following commands:
 - **scp /var/netwitness/logdecoder/packetdb/packet-0000000001.nwpdb *remote-location***
 - **scp /var/netwitness/logdecoder/metadb/meta-0000000001.nwmdb *remote-location***
 - **scp /var/netwitness/logdecoder/sessiondb/session-0000000001.nwsdb *remote-location***



NOTE: You can also copy the files from a remote location using SCP.

5. Identify the last file that was backed up by viewing the incremental back up files.

For example:

- On Day 1, if the database has **packet-0000000002.nwpdb** and **packet-0000000001.nwpdb** files, you should back up the n-1 file, **packet-0000000001.nwpdb**.
- On Day 2, back up all the files with numbers higher than **packet-0000000001.nwpdb**, with the exception of the file with the highest number.



NOTE: You can also use the file date or time to create incremental backups.

Related Documentation

- [Log Collector Database Files Overview on page 43](#)
- [Restoring Log Collector Data on page 45](#)

Restoring Log Collector Data



NOTE: Log Collector will not receive logs while data is being restored if the data is restored on the same Log Collector virtual machine that is receiving logs.

You cannot rename the backed up files while restoring data.

Ensure that the data does not overlap while you restore data to the same Log Collector. Only restore files that are not present in the directory (files that were present when the original files were rolled over).

To restore Log Collector data:

1. Manually copy or SCP the corresponding files from remote location, to all the three directories.
2. Check the size of the data to be restored and ensure that there is enough space on the system where the data will be restored.
3. Restart the service using **restart nwlogdecoder**.

Restarting the service initiates the restore process. Restore time depends on the volume of data. Original timestamps are retained once the logs are restored.



NOTE: NFS mounting of Log Collector VM directories to a remote machine is not supported.

Related Documentation

- [Log Collector Database Files Overview on page 43](#)

- [Backing Up Log Collector Data on page 44](#)