



Junos Space Security Director

Logging and Reporting Getting Started Guide

Release
13.3 R2



Published: 2014-07-27

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Copyright © 2014, 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 © 2014, 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 Notification	4
	Reports	4
	Understanding Role-Based Access Control	5
Chapter 2	Junos Space Security Director Logging and Reporting in a Virtual Environment	7
	Installation Steps Overview	7
	Prerequisites for Security Director Logging and Reporting in Virtual Environment	8
	Specifications for Deploying a Log Collector Virtual Machine on an ESX Server	9
	Installing Log Director Application on a Junos Space Network Management Platform Virtual Machine	10
	Deploying a Log Collector Virtual Machine on an ESX Server	11
	Installing Junos Space Security Director Logging and Reporting Module	12
	Adding Log Collector Virtual Machine as Special Node	13
Chapter 3	Junos Space Security Director Logging and Reporting on the JA2500 Appliance	15
	Installation Steps Overview	15
	Prerequisites for Installing Junos Space Security Director Logging and Reporting in a JA2500 Appliance	16
	Specifications for Log Director Installation on a JA2500 Appliance	17
	Installing the Log Director Application on the Junos Space Network Management Platform	17
	Installing Junos Space Security Director Logging and Reporting Module	19
	Adding the Log Collector Subsystem as a Special Node	19

Chapter 4	Log Director	21
	Log Director Overview	21
	Understanding Logging Details	21
	Understanding Log Collector Details	22
	Understanding Report Device Options	23
	Understanding Log Collector Global Settings	23
Chapter 5	Security Director and SRX Series Device Settings for Logging	25
	Configuring Security Director and SRX Series Devices to Receive Logs	25
	Configuring Security Logging	25
	Configuring Syslog	28
	Enabling Logging on Branch SRX Series Devices	30
	Enabling Logging on High End SRX Series Devices	30
Chapter 6	Back Up and Restore Log Collector Data	31
	Log Collector Database Files Overview	31
	Creating NFS Mount Point of Log Directories for Backup	32
	Mounting Log Collector Mount Point to a Remote Machine	32
	Backing up Log Collector Data	33
	Restoring Log Collector Data	34
	Forwarding System Log as Backup and Standby Option	35

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 at the Juniper Networks Technical Documentation 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 <https://www.juniper.net/cgi-bin/docbugreport/>.

- 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 JNASC 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 in a Virtual Environment on page 7](#)
- [Junos Space Security Director Logging and Reporting on the JA2500 Appliance on page 15](#)
- [Log Director on page 21](#)
- [Security Director and SRX Series Device Settings for Logging on page 25](#)
- [Back Up and Restore Log Collector Data on page 31](#)

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.

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 Notification

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 via e-mail. Reports enable you to perform trend analysis of your network activities.

Related Documentation

- [Understanding Role-Based Access Control on page 5](#)
- [Prerequisites for Security Director Logging and Reporting in Virtual Environment on page 8](#)
- [Prerequisites for Installing Junos Space Security Director Logging and Reporting in a JA2500 Appliance on page 16](#)

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 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 Security Director. Domain RBAC has the following impact on logging and reporting:

- If you have logged into 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 into the global domain, logs that do not have domain information are also displayed.
- If you have logged into 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 into the global domain, aggregated views displays logs that do not have domain information
- If you have logged into 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 into 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 into 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 into 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](#)
- [Prerequisites for Security Director Logging and Reporting in Virtual Environment on page 8](#)
- [Prerequisites for Installing Junos Space Security Director Logging and Reporting in a JA2500 Appliance on page 16](#)

CHAPTER 2

Junos Space Security Director Logging and Reporting in a Virtual Environment

The chapter covers the following topics:

- [Installation Steps Overview on page 7](#)
- [Prerequisites for Security Director Logging and Reporting in Virtual Environment on page 8](#)
- [Specifications for Deploying a Log Collector Virtual Machine on an ESX Server on page 9](#)
- [Installing Log Director Application on a Junos Space Network Management Platform Virtual Machine on page 10](#)
- [Deploying a Log Collector Virtual Machine on an ESX Server on page 11](#)
- [Installing Junos Space Security Director Logging and Reporting Module on page 12](#)
- [Adding Log Collector Virtual Machine as Special Node on page 13](#)

Installation Steps Overview

Two virtual machines are required for this deployment, which involves the following steps:

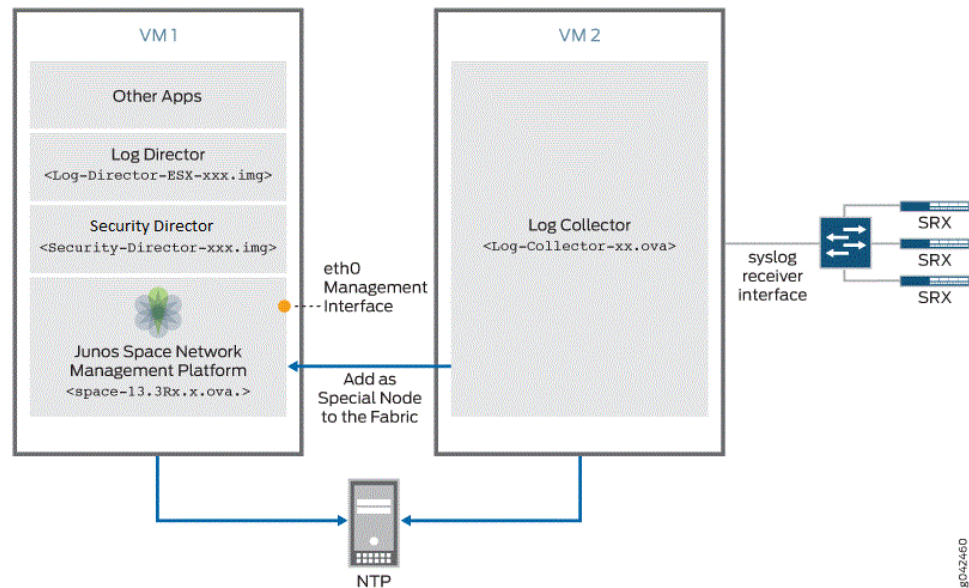
- Virtual Machine 1: Deploying the Junos Space Network Management Platform virtual machine on the ESX server. For more information see, [Junos Space Network Management Platform](#)
- [Installing Log Director Application on a Junos Space Network Management Platform Virtual Machine on page 10](#)
- Virtual Machine 2: “Deploying a Log Collector Virtual Machine on an ESX Server” on page 11.
- [Installing Junos Space Security Director Logging and Reporting Module on page 12](#)
- [Adding Log Collector Virtual Machine as Special Node on page 13](#)



NOTE: Add the Log Collector Virtual Machine as a special node after installing Log Director application.

Figure 1 on page 8 displays the Junos Space Security Director Logging and Reporting in a Virtual Environment.

Figure 1: Junos Space Security Director Logging and Reporting in a Virtual Environment



Prerequisites for Security Director Logging and Reporting in Virtual Environment

To use the Security Director Logging and Reporting module in a virtual environment, your system must meet the following prerequisites:

- The Junos Space Network Management Platform virtual machine (Virtual Machine 1) must be deployed on the ESX server. The image file can be downloaded from the download site. Example: **space-13.3R2.6.ova**.
- The Platform must be configured with Ethernet Interface eth0 and management IP addresses.
- The Platform must be up and running, and you must be able to log in to the Platform user interface.
- The following ports must be open between the space server and the Log Director VM:
 - Port 8004—Used for communication between the space and the node agent
 - Port 50102—Used for log data queries

Related Documentation

- [Understanding Junos Space Security Director Logging and Reporting on page 3](#)
- [Installation Steps Overview on page 7](#)
- [Specifications for Deploying a Log Collector Virtual Machine on an ESX Server on page 9](#)

- [Understanding How Junos Space Uses Ethernet Interfaces eth0 and eth3](#)

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

Table 3 on page 9 lists the required specifications for deploying a Log Collector virtual machine on an ESX server.

Table 3: Specifications for Deploying a Log Collector Virtual Machine on an ESX Server

Component	Specification
Memory	8 GB
Disk space	600 GB
Virtual machine file system	5.0 or later
Maximum file size	600 GB or above

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

You might experience significant performance degradation from I/O disk swapping even if you allocate the required amount of resources in your VM environment. You might experience issues with throughput and latency with a disk speed of less than 80 Mbps. Ensure that your appliance reports a minimum disk speed of 100 Mbps.

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.

```
# sync; time bash -c "(dd if=/dev/zero of=./test bs=8k count=500000; sync";
```

In the following example, the system reports a disk speed of 204 Mbps.

Example:

```
[root@NWAPPLIANCE24079 ~]# 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
```

Related Documentation

- [Understanding Junos Space Security Director Logging and Reporting on page 3](#)

- [Installation Steps Overview on page 7](#)
- [Prerequisites for Security Director Logging and Reporting in Virtual Environment on page 8](#)

Installing Log Director Application on a Junos Space Network Management Platform Virtual Machine

To install the Log Director application on the Junos Space Network Management Platform virtual machine (Virtual Machine 1):

1. Log in to the 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** and select the **Add Application** icon.

The Add Application page is displayed.

3. Using either of the following methods, upload the Log Director image.

- 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 path name of the Junos Software application file. For example: `/usr/downloads/Log-Director-JA.XX.xRx.x-VM.imgxxx.img`.
- Click **Upload**.



NOTE: The Junos Space node can be used as a server to download and store the application images.

4. To verify that **Upload Application** job is complete, click **Job ID** on the Jobs > Job Management inventory page. Wait until the job is completed and ensure that the job is successful.



NOTE: If the upload is successful, Log Director 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.

5. Click the **Add Application** icon to install the Log Director application.
Log Director is displayed in the Application page.
6. Select the Log Director image. For example: **Log-Director-ESX-xxx.img**.
7. Click **Install**.
8. Click **OK** to proceed.

The Application Management Job Information dialog box is displayed.

9. In the Application Management Job Information dialog box, click **Job ID** to view the Add Application job on the Jobs > Job Management inventory page. Wait until Log Director is fully deployed and ensure that the job is successful.
10. Log out and log in to the Junos Space Network Management Platform.

If the installation is successful, you will see a node, Logging, with sub nodes Log Collector, Reporting Devices and Global Settings displayed under Administration.

Related Documentation

- [Installation Steps Overview on page 7](#)
- [Prerequisites for Security Director Logging and Reporting in Virtual Environment on page 8](#)
- [Specifications for Deploying a Log Collector Virtual Machine on an ESX Server on page 9](#)
- [Deploying a Log Collector Virtual Machine on an ESX Server on page 11](#)

Deploying a Log Collector Virtual Machine on an ESX Server

To deploy the Log Collector virtual machine (Virtual Machine 2):

1. Download the Log Collector OVA file from the download site. Example: **Log-Collector-xxx.ova**.
2. Deploy the Log Collector OVA file on the ESX server.
3. After you complete the deployment, power on Virtual Machine 2.
4. Log in to Virtual Machine 2 using **root** as username and **juniper123** as the password.



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

5. You will be prompted to change the root password. Use the changed password while adding Virtual Machine 2 as a special node in Junos Space Network Management Platform.
6. You will also be prompted to configure the Ethernet Interface eth0 settings, which include IP address, subnet mask, and the default gateway for the Virtual Machine 2. Use this password while adding this Log Collector virtual machine as Special Node in Space Fabric



NOTE: Ensure that you can ping the Virtual Machine 2 using the configured IP address from the Space server.

Related Documentation

- [Installation Steps Overview on page 7](#)
- [Prerequisites for Security Director Logging and Reporting in Virtual Environment on page 8](#)
- [Specifications for Deploying a Log Collector Virtual Machine on an ESX Server on page 9](#)
- [Installing Log Director Application on a Junos Space Network Management Platform Virtual Machine on page 10](#)
- [NTP Time Source for a Junos Space Application.](#)
- [Using the eth0 and eth3 Ethernet Interfaces in Junos Space Overview](#)

Installing Junos Space Security Director Logging and Reporting Module

To install the Junos Space Security Director:

1. Download the latest Junos Space Security Director from the download site. For example: **Security-Director-xxx.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 and alerts nodes are displayed.



NOTE: The nodes display data when Log Director is installed and the Log Collector virtual machine is added as a special node. If Log Director is not installed the following warning is displayed: **Log Director is not installed.**

Related Documentation

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

Adding Log Collector Virtual Machine as Special Node

To add a Log Collector virtual machine (Virtual Machine 2) as a special 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** and provide the username as a **root** and the password changed after the first login.
4. Click **Add** to add the node to the fabric. Wait for the add special node job to complete.

The node is added to the fabric and updated in the database.

Log Collector node is displayed under Administration > Fabric.

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 7](#)
- [Prerequisites for Security Director Logging and Reporting in Virtual Environment on page 8](#)
- [Specifications for Deploying a Log Collector Virtual Machine on an ESX Server on page 9](#)
- [Adding a Node to the Fabric](#)

CHAPTER 3

Junos Space Security Director Logging and Reporting on the JA2500 Appliance

The Junos Space Security Director Logging and Reporting module on a JA2500 contains a single Log Director image that includes:

- Log Director application
- Log Collector subsystem within the appliance to receive logs

This chapter includes the following topics:

- [Installation Steps Overview on page 15](#)
- [Prerequisites for Installing Junos Space Security Director Logging and Reporting in a JA2500 Appliance on page 16](#)
- [Specifications for Log Director Installation on a JA2500 Appliance on page 17](#)
- [Installing the Log Director Application on the Junos Space Network Management Platform on page 17](#)
- [Installing Junos Space Security Director Logging and Reporting Module on page 19](#)
- [Adding the Log Collector Subsystem as a Special Node on page 19](#)

Installation Steps Overview

This deployment involves the following steps:

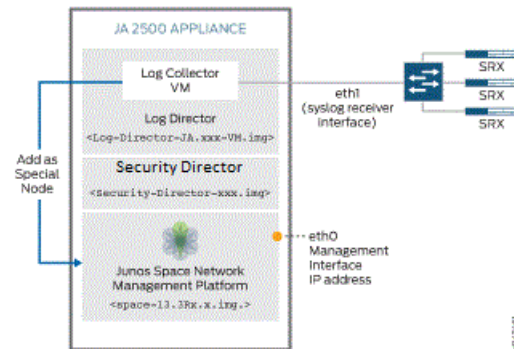
- [Installing Junos Space Network Management Platform on a JA2500 Appliance. For more information see, \[Junos Space Network Management Platform\]\(#\)](#)
- [Installing the Log Director Application on the Junos Space Network Management Platform on page 17](#)
- [Installing Junos Space Security Director Logging and Reporting Module on page 12](#)
- [Adding the Log Collector Subsystem as a Special Node on page 19](#)



NOTE: Add the Log Collector Virtual Machine as a special node after installing Log Director application.

Figure 2 on page 16 shows the setup for Junos Space Security Director Logging and Reporting in JA2500 Appliance.

Figure 2: 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 13.3 R2.6 must be installed on a JA2500 appliance from the download site. Example: **space-13.3R2.6.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 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 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 15](#)
- [Specifications for Log Director Installation on a JA2500 Appliance on page 17](#)
- [Understanding How Junos Space Uses Ethernet Interfaces eth0 and eth3](#)

Specifications for Log Director Installation on a JA2500 Appliance

Table 5 on page 17 lists the required specifications for installing the Log Collector subsystem on a JA2500 appliance that is installed as part of Log Director application installation.



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

Table 5: 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 15](#)
- [Prerequisites for Installing Junos Space Security Director Logging and Reporting in a JA2500 Appliance on page 16](#)
- [Installing the Log Director Application on the Junos Space Network Management Platform on page 17](#)

Installing the Log Director Application on the Junos Space Network Management Platform

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

1. Log in to the Platform user interface.

The box at the top of the task tree displays Network Management Platform by default.

2. Select **Network Management Platform > Administration > Applications**.
3. Click the **Add Application** icon.
4. Upload the Log Director image 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 Director 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. Select Log Director. For example: **Log-Director-JA.xxx-VM.img**.
- The option to install is displayed.
7. Click the Add Application icon to install the Log Director application.
- Log Director is displayed in the Application page.
8. Select the Log Director image.
9. Click **Install**.

The Application Configuration dialog box is displayed.

10. Enter the IP address, subnet mask, default gateway, and the password for the Log Collector subsystem.



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

11. Click **OK** to proceed.
- The Application Management Job Information dialog box appears.
12. 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.
13. 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.

- Related Documentation**
- [Installation Steps Overview on page 15](#)
 - [Prerequisites for Installing Junos Space Security Director Logging and Reporting in a JA2500 Appliance on page 16](#)
 - [Specifications for Log Director Installation on a JA2500 Appliance on page 17](#)
 - [Adding the Log Collector Subsystem as a Special Node on page 19](#)

Installing Junos Space Security Director Logging and Reporting Module

To install the Junos Space Security Director:

1. Download the latest Junos Space Security Director from the download site. For example: **Security-Director-xxx.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 and alerts nodes are displayed.



.....

NOTE: The nodes display data when Log Director is installed and the Log Collector virtual machine is added as a special node. If Log Director is not installed the following warning is displayed: **Log Director is not installed**.

.....

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

Adding the Log Collector Subsystem as a Special Node

To add the Log Collector subsystem as a special 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** and provide the password that you used while installing Log Director.
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 15](#)
- [Prerequisites for Installing Junos Space Security Director Logging and Reporting in a JA2500 Appliance on page 16](#)
- [Specifications for Log Director Installation on a JA2500 Appliance on page 17](#)
- [Adding a Node to the Fabric](#)

CHAPTER 4

Log Director

The chapter covers the following topics:

- [Log Director Overview on page 21](#)
- [Understanding Logging Details on page 21](#)
- [Understanding Log Collector Details on page 22](#)
- [Understanding Report Device Options on page 23](#)
- [Understanding Log Collector Global Settings on page 23](#)

Log Director Overview

Log Director combines the Junos Space Network Management Application Platform with a virtual machine log director component. The Junos Space Network Management Application Platform provides the options to manage and interact with the virtual machine component. The Log Director is a virtual machine an integrated solution for data storage. Log Director provides two disks, one for system data and the other for log data.

The JA2500 Junos Space Appliance provides 500 GB of space for log data storage. Log retention settings help you to manage data on the disk. If the disk usage exceeds the allocated 500 GB, the older logs will be overwritten, irrespective of the retention configuration.

Related Documentation

- [Understanding Log Collector Details on page 22](#)
- [Understanding Report Device Options on page 23](#)
- [Understanding Log Collector Global Settings on page 23](#)

Understanding Logging Details

Using logging, you can manage, license, and configure the log collector for syslog forwarding and backup . You can also view the devices that send logs. Click **Network Management Platform >Logging** to view logging details.

The Logging page lets you configure events per second (EPS) and log statistics. [Table 6 on page 22](#) provides the details of the logging parameters.

Table 6: Logging Parameters

Parameters	Details
License	
EPS License Limit	Specifies the maximum EPS per day. 500 EPS is supported currently.
Average EPS per Day	Specifies the average EPS per day. Enter the average EPS you are licensed to receive per day.
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 on a day.

Related Documentation

- [Understanding Report Device Options on page 23](#)
- [Understanding Log Collector Global Settings on page 23](#)
- [Understanding Log Collector Details on page 22](#)

Understanding Log Collector Details

The Log Collector page provides you options for viewing the log collector IP address and available free space. You can also change the database password from this page. Click **Network Management Platform > Logging > Log Collector** to view details from the log collector page.

[Table 7 on page 22](#) provides the details of the log collector parameters.

Table 7: Log Collector Parameters

Parameters	Details
General	
Collector Name	Specifies the name of the log collector.
Log Database Password	Allows you to change the password. Click Change Password to change the existing password.
Log Space Allocated	Specifies the log space allocated in the log collector.
Free Space (Log Partition)	Specifies the free space in the log collector.

Related Documentation

- [Log Director Overview on page 21](#)
- [Understanding Report Device Options on page 23](#)

- [Understanding Log Collector Global Settings on page 23](#)

Understanding Report Device Options

Click **Logging>Reporting Devices** to view device options.

[Table 8 on page 23](#) provides the details of the settings parameters on the Report Device page.

Table 8: Report Device Parameters

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 and specific device to display report device details.
Aggregate	
Device Name	Specifies the details of the device. The default details displayed are: <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	Specifies the details of the product family. The default details displayed are: <ul style="list-style-type: none"> • Product Family—Specifies the product family. • Log Count (Last 24 hours)—Specifies the log count for 24 hours.
Top Events Reporting Device Chart	Displays the chart of the reporting devices for top events.

Related Documentation

- [Log Director Overview on page 21](#)
- [Understanding Log Collector Global Settings on page 23](#)
- [Understanding Log Collector Details on page 22](#)

Understanding Log Collector Global Settings

Using log collector global settings, you can enable syslog forwarding and retention logs. Click **Network Management Platform >Logging>Global Settings** to view the log collector settings.

The Global Log Collector Settings page provides the options for syslog forwarding and for specifying the log retention period. [Table 9 on page 24](#) provides the details of the settings parameters.

Table 9: Global Log Collector Settings Parameters

Parameters	Details
Syslog Forwarding	
Enable Syslog Forwarding	<p>Allows you to enable syslog forwarding.</p> <p>Selecting the check box displays the following options:</p> <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, UDP, and TLS.
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 you have sufficient disk space to store data.</p>



NOTE: The option **Send Alerts To Queue Listeners** under **Administration>Applications>Modify Log Director Settings** is enabled by default. If you disable this option the alerts are not sent to Log Director.

Beginning 13.3 R2 you can forward subset of syslog by selecting one or more system provided categories.

Related Documentation

- [Log Director Overview on page 21](#)
- [Understanding Log Collector Details on page 22](#)
- [Understanding Report Device Options on page 23](#)

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 25](#)

Configuring Security Director and SRX Series Devices to Receive Logs

To configure syslog to receive SRX Series device logs use one of the 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 3 on page 26](#).

Figure 3: 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

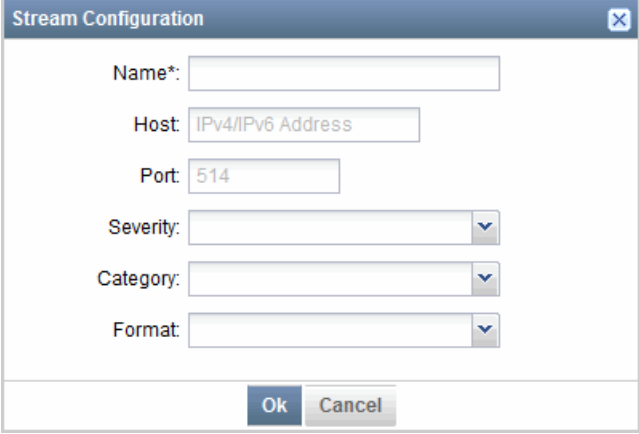
3. Under the General Settings section, configure the following parameters:
 - Mode list—Select the mode of logging as stream or event.
 - Source Address—Enter the source IP address to be used to send logs..
 - Format list—Select the logging format as **sd-syslog**.
 - Disable Logging—select the check box to disable security logging for a device.
 - UTC-Timestamp—To use Coordinated Universal Time (UTC) for security log timestamps, select the check box. (optional)
 - Event-rate—Enter the event rate to limit the rate per second at which logs are streamed.(optional)
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 4 on page 27](#).

Figure 4: 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 field—Enter the name of the new stream configuration.
- Host field—Enter the IPv4 or IPv6 address of the Log Collector.
- Port field—Enter the port number.
- Severity list—Select one of the following available required severity types:
 - Emergency
 - Alert
 - Critical
 - Error
 - Warning
 - Notice
 - Info
 - Debug
- Category list—Select the type of category as **all** or **content-security**.
- In the Format list, 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**.

Configuring Syslog

To modify syslog:

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

The Modify Syslog page appears, as shown in [Figure 5 on page 28](#).

Figure 5: Device Configuration—Modify Syslog Page

Modify Syslog

General Settings

Time-format: ☐

Source Address:

Log-Rotate-Frequency:

Allow-duplicates: ☒

Host

Name	Contents	Match	Advanced Options

File

Name	Contents	Match	Advanced Options
messages	any - any;		
default-log-messages	any - info;	{requested 'commit' operation} {copying configuration to juniper save} {commit complete} {AdminStatus} {FRU power} {FRU removal} {FRU insertion} {link UP} {transitioned} {Transferred} {transfer-file} {license add} {license delete} {package -x update} {package -x delete} GRES	Structured Data : true

Ok Cancel

2. In the General Settings section, configure the following parameters:
 - Time-format—Uncheck the check-box to include additional information in the system log time stamp.
 - 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.

- To allow the repeated messages in the system log output files, select the **Allow-duplicates** check box.
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 6 on page 29](#).

Figure 6: 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 has a large text area. The 'Contents' section has a table with two columns: 'Facility' and 'Severity'. The 'Advanced Options' section has checkboxes for 'Allow duplicates' and 'Explicit priority', a dropdown for 'Facility override', and a text field for 'Log prefix'. At the bottom are 'Ok' and 'Cancel' buttons.

- Name—elect the host name to notify.
- Under the Contents section, to configure the logging of system messages to the system console:
 - Click the plus signs (+), and the Contents page appears.
 - Facility list—from the select the message class select the class of messages to log.
 - Severity list—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 field—Specify a text string to include in each message directed to a remote destination.

- Match field—Specify a text string that must appear in a message for the message to be logged to a destination.
- Port field—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 to enable 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 to enable logging on High End SRX Series devices, see [Enable Logging on High End SRX Series Devices](#).

Related Documentation

- [Log Director Overview on page 21](#)
- [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 31](#)
- [Creating NFS Mount Point of Log Directories for Backup on page 32](#)
- [Backing up Log Collector Data on page 33](#)
- [Restoring Log Collector Data on page 34](#)
- [Forwarding System Log as Backup and Standby Option on page 35](#)

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 10 on page 31](#) provides details about the log folders.

Table 10: Log Folder Details

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

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 33](#)
- [Restoring Log Collector Data on page 34](#)
- [Forwarding Syslog as Backup and Standby Option on page 35](#)

Creating NFS Mount Point of Log Directories for Backup

To create NFS mount point of log directories for backup:

1. Log in to Log Collector VM as root **ssh root@ <Log Collector VM IP>**.
2. Ensure NFS service is operational, using the command:

service nfs status.
3. If the service is not operational, start the service using the command:

service nfs start .
4. Navigate to the location: **vi /etc/exports.**
5. Make the following entry in the file and save the file.

/var/netwitness/logdecoder/ *(ro,no_root_squash,sync).
6. Restart the NFS service using command:

service nfs status.

The following message is displayed:

```
Shutting down NFS daemon:[ OK ]
Shutting down NFS mountd:[ OK ]
Shutting down RPC idmapd:[ OK ]
Starting NFS services: [ OK ]
Starting NFS mountd: [ OK ]
Starting NFS daemon: [ OK ]
Starting RPC idmapd: [ OK ]
```

7. Navigate to **# /usr/sbin/exportfs.**

The following **/var/netwitness/logdecoder<world>** exported location and permissions are displayed.

Mounting Log Collector Mount Point to a Remote Machine

To mounting log collector mount point to a remote machine:

1. Log in to the machine to which files are to be backed up.
2. Mount **<Log Collector IP>:/var/netwitness/logdecoder -t nfs .**

3. Verify the mount using the command: **mount -l <Log Collector IP>:/var/netwitness/logdecoder on <Location where to be mounted> type nfs (rw,addr=<Log Collector IP>).**

Related Documentation

- [Backing up Log Collector Data on page 33](#)
- [Restoring Log Collector Data on page 34](#)
- [Forwarding Syslog as Backup and Standby Option on page 35](#)

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-000000001.nwpdb *remote-location***
 - **scp /var/netwitness/logdecoder/metadb/meta-000000001.nwmdb *remote-location***
 - **scp /var/netwitness/logdecoder/sessiondb/session-000000001.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 31](#)
- [Restoring Log Collector Data on page 34](#)
- [Forwarding Syslog as Backup and Standby Option on page 35](#)

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 31](#)
- [Backing up Log Collector Data on page 33](#)
- [Forwarding Syslog as Backup and Standby Option on page 35](#)

Forwarding System Log as Backup and Standby Option

Log Director provides an option to forward all system logs received by Log Collector to any remote syslog server. Use this option to instantaneously replicate data received by the Log Collector on another Log Collector VM.

To forward system logs:

1. Deploy a Log Collector VM on an ESX server using the OVA file **Log-Collector-xxx.ova**.
2. Provide a separate IP address for the deployed Log Collector VM (different from the primary Log Collector IP address).
3. Ensure that the IP address connections are established on the forwarding port 514.
4. Configure the Log Director application to forward all logs to this IP address under **Network Management Platform>Logging>Global Settings**. Specify syslog forwarding IP address, port address and category as **All Logs**.

This setup will ensure that at any time the Log Collector VM will have the same set of logs as the forwarding Log Collector.

Benefits of configuring syslog forwarding as a backup and standby option include:

1. Instantaneous replication of all the logs received at the primary Log Collector.
2. Acts as a redundant Log Collector.
3. Can be added as a special node in the space fabric and be used as the primary Log Collector to view, query and report logs.



NOTE: Only one Log Collector can be added as a special node on the Junos Space Network Management Platform Fabric.

4. Scheduled data backups occur when the disk consumption reaches a threshold.



NOTE: Configuring syslog forwarding as a backup and standby option is not a scalable solution, because it is a redundant setup with a storage constraint on the Log Collector VM of 500 GB.

Related Documentation

- [Log Collector Database Files Overview on page 31](#)
- [Backing up Log Collector Data on page 33](#)
- [Restoring Log Collector Data on page 34](#)

- [Understanding Log Collector Global Settings on page 23](#)