Junos® OS

System Log Messages Configuration Guide

Modified: 2017-06-29

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

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® OS System Log Messages Configuration Guide

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Supported Platforms

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

- M Series
- MX Series
- T Series
- PTX Series
- SRX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
     scripts {
       commit {
         file ex-script.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
   file ex-script-snippet.xsl; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see CLI Explorer.

Documentation Conventions

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

Table 1: Notice Icons

Icon	Meaning	Description
ℹ	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 xii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** ***domain-name***
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

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

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

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

Convention	Description	Examples
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at http://www.juniper.net/techpubs/feedback/.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

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

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

Junos OS System Logging

CHAPTER 1

Introduction to System Logging

Junos OS System Log Overview

The Junos OS generates system log messages (also called *syslog messages*) to record events that occur on the device, including the following:

- Routine operations, such as creation of an Open Shortest Path First (OSPF) protocol adjacency or a user login to the configuration database
- Failure and error conditions, such as failure to access a configuration file or unexpected closure of a connection to a peer process
- Emergency or critical conditions, such as router power-down due to excessive temperature

Each system log message identifies the Junos OS process that generated the message and briefly describes the operation or error that occurred. For detailed information about specific system log messages, see the *Junos OS System Log Reference for Security Devices*.

NOTE: This topic describes system log messages for Junos OS processes and libraries and not the system logging services on a Physical Interface Card (PIC) such as the Adaptive Services PIC.

Related Documentation

- Junos OS System Log Configuration Hierarchy on page 4
- Junos OS Minimum System Logging Configuration on page 6

Junos OS System Log Configuration Hierarchy

To configure the router to log system messages, include the **syslog** statement at the **[edit system]** hierarchy level:

```
[edit system]
syslog {
  archive <files number> <size size <world-readable | no-world-readable>;
  console {
    facility severity;
  }
  file filename {
    facility severity;
    archive <archive-sites {ftp-url <password password>}> <files number> <size size>
      <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
      no-world-readable>;
    explicit-priority;
    match "regular-expression";
    structured-data {
      brief;
    }
  }
  host (hostname | other-routing-engine | scc-master) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string
    match "regular-expression";
    source-address source-address;
    structured-data {
      brief;
    }
  }
  source-address source-address;
  time-format (year | millisecond | year millisecond);
  user (username | *) {
    facility severity;
    match "regular-expression";
  }
}
```

Related Documentation

- Junos OS System Log Overview on page 3

Junos OS System Logging Facilities and Message Severity Levels

Table 3 on page 5 lists the Junos OS system logging facilities that you can specify in configuration statements at the **[edit system syslog]** hierarchy level.

Table 3: Junos OS System Logging Facilities

Facility	Type of Event or Error
any	All (messages from all facilities)
authorization	Authentication and authorization attempts
change-log	Changes to the Junos OS configuration
conflict-log	Specified configuration is invalid on the router type
daemon	Actions performed or errors encountered by system processes
dfc	Events related to dynamic flow capture
explicit-priority	Include priority and facility in system log messages.
external	Actions performed or errors encountered by the local external applications.
firewall	Packet filtering actions performed by a firewall filter
ftp	Actions performed or errors encountered by the FTP process
interactive-commands	Commands issued at the Junos OS command-line interface (CLI) prompt or by a client application such as a Junos XML protocol or NETCONF XML client
kernel	Actions performed or errors encountered by the Junos OS kernel
ntp	Actions performed or errors encountered by the Network Time Protocol processes.
pfe	Actions performed or errors encountered by the Packet Forwarding Engine
security	Security related events or errors.
user	Actions performed or errors encountered by user-space processes

Table 4 on page 5 lists the severity levels that you can specify in configuration statements at the **[edit system syslog]** hierarchy level. The levels from **emergency** through **info** are in order from highest severity (greatest effect on functioning) to lowest.

Unlike the other severity levels, the **none** level disables logging of a facility instead of indicating how seriously a triggering event affects routing functions. For more information, see “Disabling the System Logging of a Facility” on page 28.

Table 4: System Log Message Severity Levels

Value	Severity Level	Description
N/A	**none**	Disables logging of the associated facility to a destination

Table 4: System Log Message Severity Levels *(continued)*

Value	Severity Level	Description
0	**emergency**	System panic or other condition that causes the router to stop functioning
1	**alert**	Conditions that require immediate correction, such as a corrupted system database
2	**critical**	Critical conditions, such as hard errors
3	**error**	Error conditions that generally have less serious consequences than errors at the emergency, alert, and critical levels
4	**warning**	Conditions that warrant monitoring
5	**notice**	Conditions that are not errors but might warrant special handling
6	**info**	Events or nonerror conditions of interest
7	**any**	Includes all severity levels

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 13
- Examples: Configuring System Logging on page 29

Junos OS Minimum System Logging Configuration

To record or view system log messages, you must include the **syslog** statement at the **[edit system]** hierarchy level. Specify at least one destination for the messages, as described in Table 5 on page 6. For more information about the configuration statements, see “Single-Chassis System Logging Configuration Overview” on page 13.

Table 5: Minimum Configuration Statements for System Logging

Destination	Minimum Configuration Statements

File	[edit system syslog]
	file *filename* {
	  facility severity;
	}

Terminal session of one, several, or all users	[edit system syslog]
	user (*username* | *) {
	  facility severity;
	}

Router or switch console	[edit system syslog]
	console {
	  facility severity;
	}

Table 5: Minimum Configuration Statements for System Logging *(continued)*

Destination	Minimum Configuration Statements

Remote machine or the other Routing Engine on the router or switch	[edit system syslog]
	host (*hostname* | other-routing-engine) {
	facility *severity*;
	}

Related Documentation

- Junos OS System Log Overview on page 3

Junos OS Default System Log Settings

Table 6 on page 7 summarizes the default system log settings that apply to all routers that run the Junos OS, and specifies which statement to include in the configuration to override the default value.

Table 6: Default System Logging Settings

Setting	Default	Overriding Statement	Instructions

Alternative facility for message forwarded to a remote machine	For **change-log**: **local6**
	For **conflict-log**: **local5**
	For **dfc**: **local1**
	For **firewall**: **local3**
	For **interactive-commands**: **local7**
	For **pfe**: **local4**
		[edit system syslog]
		host *hostname* {
		facility-override *facility*;
		}
			"Changing the Alternative Facility Name for System Log Messages Directed to a Remote Destination" on page 33

Format of messages logged to a file	Standard Junos OS format, based on UNIX format	[edit system syslog]
		file *filename* {
		structured-data;
		}
			"Logging Messages in Structured-Data Format" on page 18

Maximum number of files in the archived set	10	[edit system syslog]
		archive {
		files *number*;
		}
		file *filename* {
		archive {
		files *number*;
		}
		}
			"Specifying Log File Size, Number, and Archiving Properties" on page 19

Table 6: Default System Logging Settings *(continued)*

Setting	Default	Overriding Statement	Instructions

Maximum size of the log file	M Series, MX Series, and T Series: 1 megabyte (MB)
	TX Matrix: 10 MB
		[edit system syslog]
		archive {
		  size *size*;
		}
		file *filename* {
		  archive {
		    size *size*;
		  }
		}
			"Specifying Log File Size, Number, and Archiving Properties" on page 19

Timestamp format	Month, date, hour, minute, second For example: **Aug 21 12:36:30**	[edit system syslog] time-format *format*;	"Including the Year or Millisecond in Timestamps" on page 24

Users who can read log files	**root** user and users with the Junos OS **maintenance** permission	[edit system syslog]
		archive {
		  world-readable;
		}
		file *filename* {
		  archive {
		    world-readable;
		  }
		}
			"Specifying Log File Size, Number, and Archiving Properties" on page 19

- Junos OS System Log Overview on page 3
- Junos OS Platform-Specific Default System Log Messages on page 8

Junos OS Platform-Specific Default System Log Messages

The following messages are generated by default on specific routers. To view any of these types of messages, you must configure at least one destination for messages as described in "Junos OS Minimum System Logging Configuration" on page 6.

- To log the kernel process message on an M Series, MX Series, or T Series router, include the **kernel info** statement at the appropriate hierarchy level:

  ```
  [edit system syslog]
  (console | file filename | host destination | user username) {
    kernel info;
  }
  ```

- On a routing matrix composed of a TX Matrix router and T640 routers, the master Routing Engine on each T640 router forwards all messages with a severity of **info** and higher to the master Routing Engine on the TX Matrix router. This is equivalent to the following configuration statement included on the TX Matrix router:

  ```
  [edit system syslog]
  host scc-master {
    any info;
  }
  ```

- Starting in Junos OS Release 15.1X49-D10, likewise on a routing matrix composed of a TX Matrix Plus router with connected T1600 or T4000 routers, the master Routing Engine on each T1600 or T4000 LCC forwards to the master Routing Engine on the TX Matrix Plus router all messages with a severity of **info** and higher. This is equivalent to the following configuration statement included on the TX Matrix Plus router:

  NOTE: From the perspective of the user interface, the routing matrix appears as a single router. The TX Matrix Plus router controls all the T1600 or T4000 routers connected to it in the routing matrix.

```
[edit system syslog]
host sfc0-master {
   any info;
}
```

Release History Table

Release	Description
15.1X49-D10	Starting in Junos OS Release 15.1X49-D10, likewise on a routing matrix composed of a TX Matrix Plus router with connected T1600 or T4000 routers, the master Routing Engine on each T1600 or T4000 LCC forwards to the master Routing Engine on the TX Matrix Plus router all messages with a severity of **info** and higher.

Related Documentation

- Junos OS System Log Overview on page 3
- Junos OS Default System Log Settings on page 7
- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

PART 2

Security Logging

CHAPTER 2

Configuring System Logging for a Single-Chassis System

Single-Chassis System Logging Configuration Overview

The Junos system logging utility is similar to the UNIX **syslogd** utility. This section describes how to configure system logging for a single-chassis system that runs the Junos OS.

System logging configuration for the Junos-FIPS software and for Juniper Networks routers in a Common Criteria environment is the same as for the Junos OS. For more information, see the *Secure Configuration Guide for Common Criteria and Junos-FIPS*.

For information about configuring system logging for a routing matrix composed of a TX Matrix router and T640 routers, see “Configuring System Logging for a TX Matrix Router” on page 39.

Each system log message belongs to a *facility*, which groups together related messages. Each message is also preassigned a *severity level*, which indicates how seriously the triggering event affects router functions. You always specify the facility and severity of the messages to include in the log. For more information, see "Specifying the Facility and Severity of Messages to Include in the Log" on page 15.

You direct messages to one or more destinations by including the appropriate statement at the **[edit system syslog]** hierarchy level:

- To a named file in a local file system, by including the **file** statement. See "Directing System Log Messages to a Log File" on page 17.
- To the terminal session of one or more specific users (or all users) when they are logged in to the router, by including the **user** statement. See "Directing System Log Messages to a User Terminal" on page 18.
- To the router console, by including the **console** statement. See "Directing System Log Messages to the Console" on page 19.
- To a remote machine that is running the **syslogd** utility or to the other Routing Engine on the router, by including the **host** statement. See "Directing System Log Messages to a Remote Machine or the Other Routing Engine" on page 31.

By default, messages are logged in a standard format, which is based on a UNIX system log format; for detailed information about message formatting, see the System Log Explorer. You can alter the content and format of logged messages in the following ways:

- You can log messages to a file in structured-data format instead of the standard Junos format. Structured-data format provides more information without adding significant length, and makes it easier for automated applications to extract information from the message. For more information, see "Logging Messages in Structured-Data Format" on page 18.
- A message's facility and severity level are together referred to as its *priority*. By default, the standard Junos format for messages does not include priority information (structured-data format includes a priority code by default.) To include priority information in standard-format messages directed to a file or a remote destination, include the **explicit-priority** statement. For more information, see "Including Priority Information in System Log Messages" on page 21.
- By default, the standard Junos format for messages specifies the month, date, hour, minute, and second when the message was logged. You can modify the timestamp on standard-format system log messages to include the year, the millisecond, or both. (Structured-data format specifies the year and millisecond by default.) For more information, see "Including the Year or Millisecond in Timestamps" on page 24.
- When directing messages to a remote machine, you can specify the IP address that is reported in messages as their source. You can also configure features that make it easier to separate messages generated by the Junos OS or messages generated on particular routers. For more information, see "Directing System Log Messages to a Remote Machine or the Other Routing Engine" on page 31.
- The predefined facilities group together related messages, but you can also use regular expressions to specify more exactly which messages from a facility are logged to a

file, a user terminal, or a remote destination. For more information, see “Using Regular Expressions to Refine the Set of Logged Messages” on page 25.

Related Documentation

- Examples: Configuring System Logging on page 29
- Specifying the Facility and Severity of Messages to Include in the Log on page 15
- Junos OS System Logging Facilities and Message Severity Levels on page 4
- Directing System Log Messages to a Log File on page 17
- Directing System Log Messages to a User Terminal on page 18
- Directing System Log Messages to the Console on page 19
- Directing System Log Messages to a Remote Machine or the Other Routing Engine on page 31

Specifying the Facility and Severity of Messages to Include in the Log

Each system log message belongs to a facility, which groups together messages that either are generated by the same source (such as a software process) or concern a similar condition or activity (such as authentication attempts). Each message is also preassigned a *severity level*, which indicates how seriously the triggering event affects routing platform functions.

When you configure logging for a facility and destination, you specify a severity level for each facility. Messages from the facility that are rated at that level and higher are logged to the following destination:

```
[edit system syslog]
(console | file filename | host destination | user username) {
 facility severity ;
}
```

For more information about the destinations, see “Directing System Log Messages to a User Terminal” on page 18, and, “Directing System Log Messages to the Console” on page 19.

To log messages belonging to more than one facility to a particular destination, specify each facility and associated severity as a separate statement within the set of statements for the destination.

Table 3 on page 5 lists the Junos OS system logging facilities that you can specify in configuration statements at the **[edit system syslog]** hierarchy level.

Table 7: Junos OS System Logging Facilities

Facility	Type of Event or Error
any	All (messages from all facilities)
authorization	Authentication and authorization attempts

Table 7: Junos OS System Logging Facilities *(continued)*

Facility	Type of Event or Error
change-log	Changes to the Junos OS configuration
conflict-log	Specified configuration is invalid on the router type
daemon	Actions performed or errors encountered by system processes
dfc	Events related to dynamic flow capture
firewall	Packet filtering actions performed by a firewall filter
ftp	Actions performed or errors encountered by the FTP process
interactive-commands	Commands issued at the Junos OS command-line interface (CLI) prompt or by a client application such as a Junos XML protocol or NETCONF XML client
kernel	Actions performed or errors encountered by the Junos OS kernel
pfe	Actions performed or errors encountered by the Packet Forwarding Engine
user	Actions performed or errors encountered by user-space processes

Table 4 on page 5 lists the severity levels that you can specify in configuration statements at the **[edit system syslog]** hierarchy level. The levels from **emergency** through **info** are in order from highest severity (greatest effect on functioning) to lowest.

Unlike the other severity levels, the **none** level disables logging of a facility instead of indicating how seriously a triggering event affects routing functions. For more information, see "Disabling the System Logging of a Facility" on page 28.

Table 8: System Log Message Severity Levels

Value	Severity Level	Description
N/A	**none**	Disables logging of the associated facility to a destination
0	**emergency**	System panic or other condition that causes the router to stop functioning
1	**alert**	Conditions that require immediate correction, such as a corrupted system database
2	**critical**	Critical conditions, such as hard errors
3	**error**	Error conditions that generally have less serious consequences than errors at the emergency, alert, and critical levels
4	**warning**	Conditions that warrant monitoring

Table 8: System Log Message Severity Levels *(continued)*

Value	Severity Level	Description
5	**notice**	Conditions that are not errors but might warrant special handling
6	**info**	Events or nonerror conditions of interest
7	**any**	Includes all severity levels

Related Documentation

- Junos OS System Logging Facilities and Message Severity Levels on page 4
- Single-Chassis System Logging Configuration Overview on page 13
- Examples: Configuring System Logging on page 29

Directing System Log Messages to a Log File

To direct system log messages to a file in the **/var/log** directory of the local Routing Engine, include the **file** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
file filename {
  facility severity;
  archive <archive-sites (ftp-url <password password>)> <files number> <size size>
    <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
    no-world-readable>;
  explicit-priority;
  match "regular-expression";
  structured-data {
    brief;
  }
}
```

For the list of facilities and severity levels, see “Specifying the Facility and Severity of Messages to Include in the Log” on page 15.

To prevent log files from growing too large, the Junos OS system logging utility by default writes messages to a sequence of files of a defined size. By including the **archive** statement, you can configure the number of files, their maximum size, and who can read them, either for all log files or for a certain log file. For more information, see “Specifying Log File Size, Number, and Archiving Properties” on page 19.

For information about the following statements, see the indicated sections:

- **explicit-priority**—See “Including Priority Information in System Log Messages” on page 21
- **match**—See “Using Regular Expressions to Refine the Set of Logged Messages” on page 25
- **structured-data**—See “Logging Messages in Structured-Data Format” on page 18

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 13
- *Overview of Junos OS System Log Messages*
- Logging Messages in Structured-Data Format on page 18
- Examples: Configuring System Logging on page 29

Logging Messages in Structured-Data Format

You can log messages to a file in structured-data format instead of the standard Junos OS format. Structured-data format provides more information without adding significant length, and makes it easier for automated applications to extract information from a message.

The structured-data format complies with Internet draft draft-ietf-syslog-protocol-23, *The syslog Protocol*, which is at http://tools.ietf.org/html/draft-ietf-syslog-protocol-23. The draft establishes a standard message format regardless of the source or transport protocol for logged messages.

To output messages to a file in structured-data format, include the **structured-data** statement at the **[edit system syslog file *filename*]** hierarchy level:

```
[edit system syslog file filename]
facility severity;
structured-data {
   brief;
}
```

The optional **brief** statement suppresses the English-language text that appears by default at the end of a message to describe the error or event.

The structured format is used for all messages logged to the file that are generated by a Junos process or software library.

NOTE: If you include either or both of the **explicit-priority** and **time-format** statements along with the **structured-data** statement, they are ignored. These statements apply to the standard Junos OS system log format, not to structured-data format.

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 13
- Examples: Configuring System Logging on page 29

Directing System Log Messages to a User Terminal

To direct system log messages to the terminal session of one or more specific users (or all users) when they are logged in to the local Routing Engine, include the **user** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
user (username | *) {
   facility severity;
   match "regular-expression";
}
```

Specify one or more Junos OS usernames, separating multiple values with spaces, or use the asterisk (*) to indicate all users who are logged in to the local Routing Engine.

For the list of logging facilities and severity levels, see "Specifying the Facility and Severity of Messages to Include in the Log" on page 15. For information about the **match** statement, see "Using Regular Expressions to Refine the Set of Logged Messages" on page 25.

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 13
- Examples: Configuring System Logging on page 29

Directing System Log Messages to the Console

To direct system log messages to the console of the local Routing Engine, include the **console** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
console {
   facility severity;
}
```

For the list of logging facilities and severity levels, see "Specifying the Facility and Severity of Messages to Include in the Log" on page 15.

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 13
- Examples: Configuring System Logging on page 29

Specifying Log File Size, Number, and Archiving Properties

To prevent log files from growing too large, by default the Junos OS system logging utility writes messages to a sequence of files of a defined size. The files in the sequence are referred to as *archive* files to distinguish them from the *active* file to which messages are currently being written. The default maximum size depends on the platform type:

- 128 kilobytes (KB) for EX Series switches
- 1 megabyte (MB) for M Series, MX Series, and T Series routers
- 10 MB for TX Matrix or TX Matrix Plus routers
- 1 MB for the QFX Series

When an active log file called ***logfile*** reaches the maximum size, the logging utility closes the file, compresses it, and names the compressed archive file ***logfile*.0.gz**. The logging utility then opens and writes to a new active file called ***logfile***. This process is also known as file rotation. When the new ***logfile*** reaches the configured maximum size, ***logfile*.0.gz** is renamed ***logfile*.1.gz**, and the new ***logfile*** is closed, compressed, and renamed ***logfile*.0.gz**. By default, the logging utility creates up to 10 archive files in this manner. When the maximum number of archive files is reached and when the size of the active file reaches the configured maximum size, the contents of the last archived file are overwritten by the current active file. The logging utility by default also limits the users who can read log files to the **root** user and users who have Junos OS **maintenance** permission.

Junos OS provides a configuration statement **log-rotate-frequency** that configures the system log file rotation frequency by configuring the time interval for checking the log file size. The frequency can be set to a value of 1 minute through 59 minutes. The default frequency is 15 minutes.

To configure the log rotation frequency, include the **log-rotate-frequency** statement at the **[edit system syslog]** hierarchy level.

You can include the **archive** statement to change the maximum size of each file, how many archive files are created, and who can read log files.

To configure values that apply to all log files, include the **archive** statement at the **[edit system syslog]** hierarchy level:

```
archive <files number> <size size> <world-readable | no-world-readable>;
```

To configure values that apply to a specific log file, include the **archive** statement at the **[edit system syslog file *filename*]** hierarchy level:

```
archive <archive-sites (ftp-url <password password>)> <files number> <size size>
  <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
  no-world-readable> ;
```

archive-sites *site-name* specifies a list of archive sites that you want to use for storing files. The ***site-name*** value is any valid FTP URL to a destination. If more than one site name is configured, a list of archive sites for the system log files is created. When a file is archived, the router or switch attempts to transfer the file to the first URL in the list, moving to the next site only if the transfer does not succeed. The log file is stored at the archive site with the specified log filename. For information about how to specify valid FTP URLs, see Format for Specifying Filenames and URLs in Junos OS CLI Commands.

binary-data Mark file as containing binary data. This allows proper archiving of binary files, such as WTMP files (login records for UNIX based systems). To restore the default setting, include the **no-binary-data** statement.

files *number* specifies the number of files to create before the oldest file is overwritten. The value can be from 1 through 1000.

size *size* specifies the maximum size of each file. The value can be from 64 KB (64k) through 1 gigabyte (1g); to represent megabytes, use the letter **m** after the integer. There is no space between the digits and the **k**, **m**, or **g** units letter.

start-time "*YYYY-MM-DD.hh:mm*" defines the date and time in the local time zone for a one-time transfer of the active log file to the first reachable site in the list of sites specified by the **archive-sites** statement.

transfer-interval *interval* defines the amount of time the current log file remains open (even if it has not reached the maximum possible size) and receives new statistics before it is closed and transferred to an archive site. This interval value can be from 5 through 2880 minutes.

world-readable enables all users to read log files. To restore the default permissions, include the **no-world-readable** statement.

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 13
- Examples: Configuring System Logging on page 29
- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

Including Priority Information in System Log Messages

The facility and severity level of a message are together referred to as its *priority*. By default, messages logged in the standard Junos OS format do not include information about priority. To include priority information in standard-format messages directed to a file, include the **explicit-priority** statement at the **[edit system syslog file *filename*]** hierarchy level:

```
[edit system syslog file filename]
facility severity;
explicit-priority;
```

NOTE: Messages logged in structured-data format include priority information by default. If you include the **structured-data** statement at the **[edit system syslog file *filename*]** hierarchy level along with the **explicit-priority** statement, the **explicit-priority** statement is ignored and messages are logged in structured-data format.

For information about the **structured-data** statement, see "Logging Messages in Structured-Data Format" on page 18. For information about the contents of a structured-data message, see the *Junos OS System Log Reference for Security Devices*.

To include priority information in messages directed to a remote machine or the other Routing Engine, include the **explicit-priority** statement at the **[edit system syslog host (*hostname* | other-routing-engine)]** hierarchy level:

```
[edit system syslog host (hostname | other-routing-engine)]
facility severity;
explicit-priority;
```

NOTE: The **other-routing-engine** option does not apply to the QFX Series.

The priority recorded in a message always indicates the original, local facility name. If the **facility-override** statement is included for messages directed to a remote destination, the Junos OS system logging utility still uses the alternative facility name for the messages themselves when directing them to the remote destination. For more information, see "Changing the Alternative Facility Name for System Log Messages Directed to a Remote Destination" on page 33.

When the **explicit-priority** statement is included, the Junos OS logging utility prepends codes for the facility name and severity level to the message tag name, if the message has one:

```
FACILITY-severity[-TAG]
```

(The tag is a unique identifier assigned to some Junos OS system log messages.)

In the following example, the **CHASSISD_PARSE_COMPLETE** message belongs to the **daemon** facility and is assigned severity **info** (6):

```
Aug 21 12:36:30 router1 chassisd[522]: %DAEMON-6-CHASSISD_PARSE_COMPLETE:
   Using new configuration
```

When the **explicit-priority** statement is not included, the priority does not appear in the message:

```
Aug 21 12:36:30 router1 chassisd[522]: CHASSISD_PARSE_COMPLETE: Using new
   configuration
```

For more information about message formatting, see the *Junos OS System Log Reference for Security Devices*.

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 13
- Examples: Configuring System Logging on page 29

System Log Facility Codes and Numerical Codes Reported in Priority Information

Table 9 on page 22 lists the facility codes that can appear in system log messages and maps them to facility names.

NOTE: If the second column in Table 9 on page 22 does not include the Junos OS facility name for a code, the facility cannot be included in a statement at the **[edit system syslog]** hierarchy level. Junos OS might use the facilities in Table 9 on page 22—and others that are not listed—when reporting on internal operations.

Table 9: Facility Codes Reported in Priority Information

Code	Junos Facility Name	Type of Event or Error
AUTH	**authorization**	Authentication and authorization attempts

Table 9: Facility Codes Reported in Priority Information *(continued)*

Code	Junos Facility Name	Type of Event or Error
AUTHPRIV		Authentication and authorization attempts that can be viewed by superusers only
CHANGE	change-log	Changes to Junos OS configuration
CONFLICT	conflict-log	Specified configuration is invalid on the router type
CONSOLE		Messages written to **/dev/console** by the kernel console output r
CRON		Actions performed or errors encountered by the cron process
DAEMON	daemon	Actions performed or errors encountered by system processes
DFC	dfc	Actions performed or errors encountered by the dynamic flow capture process
FIREWALL	firewall	Packet filtering actions performed by a firewall filter
FTP	ftp	Actions performed or errors encountered by the FTP process
INTERACT	interactive-commands	Commands issued at the Junos OS CLI prompt or invoked by a client application such as a Junos XML protocol or NETCONF client
KERN	kernel	Actions performed or errors encountered by the Junos kernel
NTP		Actions performed or errors encountered by the Network Time Protocol (NTP)
PFE	pfe	Actions performed or errors encountered by the Packet Forwarding Engine
SYSLOG		Actions performed or errors encountered by the Junos system logging utility
USER	user	Actions performed or errors encountered by user-space processes

Table 10 on page 24 lists the numerical severity codes that can appear in system log messages and maps them to severity levels.

Table 10: Numerical Codes for Severity Levels Reported in Priority Information

Numerical Code	Severity Level	Description
0	**emergency**	System panic or other condition that causes the router to stop functioning
1	**alert**	Conditions that require immediate correction, such as a corrupted system database
2	**critical**	Critical conditions, such as hard errors
3	**error**	Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels
4	**warning**	Conditions that warrant monitoring
5	**notice**	Conditions that are not errors but might warrant special handling
6	**info**	Events or nonerror conditions of interest
7	**debug**	Software debugging messages (these appear only if a technical support representative has instructed you to configure this severity level)

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 13
- Examples: Configuring System Logging on page 29

Including the Year or Millisecond in Timestamps

By default, the timestamp recorded in a standard-format system log message specifies the month, date, hour, minute, and second when the message was logged, as in the following example:

```
Aug 21 12:36:30
```

To include the year, the millisecond, or both in the timestamp, include the **time-format** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
time-format (year | millisecond | year millisecond);
```

However, the timestamp for traceoption messages is specified in milliseconds by default, and is independent of the **[edit system syslog time-format]** statement.

The modified timestamp is used in messages directed to each destination configured by a **file**, **console**, or **user** statement at the **[edit system syslog]** hierarchy level, but not to destinations configured by a **host** statement.

NOTE: By default, in a FreeBSD console, the additional time information is not available in system log messages directed to each destination configured by a **host** statement. However, in a Junos OS specific implementation using the FreeBSD console, the additional time information is available in system log messages directed to each destination.

The following example illustrates the format for a timestamp that includes both the millisecond (401) and the year (2006):

```
Aug 21 12:36:30.401 2006
```

NOTE: Messages logged in structured-data format include the year and millisecond by default. If you include the structured-data statement at the **[edit system syslog file *filename*]** hierarchy level along with the **time-format** statement, the **time-format** statement is ignored and messages are logged in structured-data format.

For information about the **structured-data** statement, see "Logging Messages in Structured-Data Format" on page 18. For information about the contents of a structured-data message, see the *Junos OS System Log Reference for Security Devices*.

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 13
- Examples: Configuring System Logging on page 29

Using Regular Expressions to Refine the Set of Logged Messages

The predefined facilities group together related messages, but you can also use regular expression matching to specify more exactly which messages from a facility are logged to a file, a user terminal, or a remote destination.

Starting with Junos OS Release 16.1, to specify the text string that must (or must not) appear in a message for the message to be logged to a destination, include the **match** and the **match-string** statements Specify the regular expression which the text string must match:

```
match "regular-expression";
```

To specify the text substring that must appear in a message for the message to be logged to a destination, include the **match-string** statement and specify the regular expression which the text substring must match:

```
match-string <string-name>;
```

You can include this statement at the following hierarchy levels:

- **[edit system syslog file *filename*]** (for a file)

- **[edit system syslog user (*username* | *)]** (for a specific user session or for all user sessions on a terminal)
- **[edit system syslog host (*hostname* | other-routing-engine)]** (for a remote destination)

In specifying the regular expression, use the notation defined in POSIX Standard 1003.2 for extended (modern) UNIX regular expressions. Explaining regular expression syntax is beyond the scope of this document, but POSIX standards are available from the Institute of Electrical and Electronics Engineers (IEEE, http://www.ieee.org).

Table 11 on page 26 specifies which character or characters are matched by some of the regular expression operators that you can use in the match statement. In the descriptions, the term term refers to either a single alphanumeric character or a set of characters enclosed in square brackets, parentheses, or braces.

NOTE: **The match statement is not case-sensitive.**

Table 11: Regular Expression Operators for the match Statement

Operator	Matches
. (period)	One instance of any character except the space.
* (asterisk)	Zero or more instances of the immediately preceding term.
+ (plus sign)	One or more instances of the immediately preceding term.
? (question mark)	Zero or one instance of the immediately preceding term.
| (pipe)	One of the terms that appears on either side of the pipe operator.
! (exclamation point)	Any string except the one specified by the expression, when the exclamation point appears at the start of the expression. Use of the exclamation point is Junos OS-specific.
ˆ (caret)	Start of a line, when the caret appears outside square brackets. One instance of any character that does not follow it within square brackets, when the caret is the first character inside square brackets.
$ (dollar sign)	End of a line.
[ ] (paired square brackets)	One instance of one of the enclosed alphanumeric characters. To indicate a range of characters, use a hyphen (-) to separate the beginning and ending characters of the range. For example, [a-z0-9] matches any letter or number.
( ) (paired parentheses)	One instance of the evaluated value of the enclosed term. Parentheses are used to indicate the order of evaluation in the regular expression.

Using Regular Expressions

Filter messages that belong to the **interactive-commands** facility, directing those that include the string **configure** to the terminal of the root user:

```
[edit system syslog]
user root {
 interactive-commands any;
 match “.*configure.*”;
}
```

Messages like the following appear on the **root** user’s terminal when a user issues a **configure** command to enter configuration mode:

timestamp *router-name* mgd[PID]: UI_CMDLINE_READ_LINE: User '*user*', command 'configure private'

Filter messages that belong to the **daemon** facility and have a severity of **error** or higher, directing them to the file **/var/log/process-errors**. Omit messages generated by the SNMP process (snmpd), instead directing them to the file **/var/log/snmpd-errors**:

```
[edit system syslog]
file process-errors {
 daemon error;
 match “!(.*snmpd.*)”;
}
file snmpd-errors {
 daemon error;
 match “.*snmpd.*”;
}
```

Release History Table

Release	Description
16.1	Starting with Junos OS Release 16.1, to specify the text string that must (or must not) appear in a message for the message to be logged to a destination, include the **match** and the **match-string** statements

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 13
- Examples: Configuring System Logging on page 29

Junos System Log Regular Expression Operators for the match Statement

Table 12: Regular Expression Operators for the match Statement

Operator	Matches
. (period)	One instance of any character except the space.
***** (asterisk)	Zero or more instances of the immediately preceding term.
+ (plus sign)	One or more instances of the immediately preceding term.
? (question mark)	Zero or one instance of the immediately preceding term.

Table 12: Regular Expression Operators for the match Statement *(continued)*

Operator	Matches
| (pipe)	One of the terms that appear on either side of the pipe operator.
! (exclamation point)	Any string except the one specified by the expression, when the exclamation point appears at the start of the expression. Use of the exclamation point is Junos OS–specific.
^ (caret)	The start of a line, when the caret appears outside square brackets. One instance of any character that does not follow it within square brackets, when the caret is the first character inside square brackets.
$ (dollar sign)	The end of a line.
[ ] (paired square brackets)	One instance of one of the enclosed alphanumeric characters. To indicate a range of characters, use a hyphen (**-**) to separate the beginning and ending characters of the range. For example, **[a-z0-9]** matches any letter or number.
( ) (paired parentheses)	One instance of the evaluated value of the enclosed term. Parentheses are used to indicate the order of evaluation in the regular expression.

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 13
- Examples: Configuring System Logging on page 29

Disabling the System Logging of a Facility

To disable the logging of messages that belong to a particular facility, include the ***facility*** **none** statement in the configuration. This statement is useful when, for example, you want to log messages that have the same severity level and belong to all but a few facilities. Instead of including a statement for each facility you want to log, you can include the **any** ***severity*** statement and then a ***facility*** **none** statement for each facility that you do not want to log. For example, the following logs all messages at the **error** level or higher to the console, except for messages from the **daemon** and **kernel** facilities. Messages from those facilities are logged to the file **>/var/log/internals** instead:

```
[edit system syslog]
console {
    any error;
    daemon none;
    kernel none;
}
file internals {
    daemon info;
    kernel info;
}
```

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 13

Examples: Configuring System Logging

The following example shows how to configure the logging of messages about all commands entered by users at the CLI prompt or invoked by client applications such as Junos OS XML protocol or NETCONF client applications, and all authentication or authorization attempts, both to the file **cli-commands** and to the terminal of any user who is logged in:

```
[edit system]
syslog {
   file cli-commands {
      interactive-commands info;
      authorization info;
   }
   user * {
      interactive-commands info;
      authorization info;
   }
}
```

The following example shows how to configure the logging of all changes in the state of alarms to the file **/var/log/alarms**:

```
[edit system]
syslog {
   file alarms {
      kernel warning;
   }
}
```

The following example shows how to configure the handling of messages of various types, as described in the comments. Information is logged to two files, to the terminal of user **alex**, to a remote machine, and to the console:

```
[edit system]
syslog {
   /* write all security-related messages to file /var/log/security */
   file security {
      authorization info;
      interactive-commands info;
   }
   /* write messages about potential problems to file /var/log/messages: */
   /* messages from "authorization" facility at level "notice" and above, */
   /* messages from all other facilities at level "warning" and above */
   file messages {
      authorization notice;
      any warning;
   }
   /* write all messages at level "critical" and above to terminal of user "alex" if */
   /* that user is logged in */
   user alex {
      any critical;
```

```
    }
    /* write all messages from the "daemon" facility at level "info" and above, and */
    /* messages from all other facilities at level "warning" and above, to the */
    /* machine monitor.mycompany.com */
    host monitor.mycompany.com {
        daemon info;
        any warning;
    }
    /* write all messages at level "error" and above to the system console */
    console {
        any error;
    }
}
```

The following example shows how to configure the handling of messages generated when users issue Junos OS CLI commands, by specifying the **interactive-commands** facility at the following severity levels:

- **info**—Logs a message when users issue any command at the CLI operational or configuration mode prompt. The example writes the messages to the file **/var/log/user-actions**.
- **notice**—Logs a message when users issue the configuration mode commands **rollback** and **commit**. The example writes the messages to the terminal of user **philip**.
- **warning**—Logs a message when users issue a command that restarts a software process. The example writes the messages to the console.

```
[edit system]
syslog {
    file user-actions {
        interactive-commands info;
    }
    user philip {
        interactive-commands notice;
    }
    console {
        interactive-commands warning;
    }
}
```

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 13

CHAPTER 3

Directing System Log Messages to a Remote Destination

Directing System Log Messages to a Remote Machine or the Other Routing Engine

To direct system log messages to a remote machine or to the other Routing Engine on the router, include the **host** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
host (hostname | other-routing-engine) {
  facility severity;
  explicit-priority;
  facility-override facility;
  log-prefix string;
  match "regular-expression";
  source-address source-address;
  structured-data {
    brief;
  }
}
source-address source-address;
```

To direct system log messages to a remote machine, include the **host** ***hostname*** statement to specify the remote machine's IP version 4 (IPv4) address, IP version 6 (IPv6) address, or fully qualified hostname. The remote machine must be running the standard **syslogd** utility. We do not recommend directing messages to another Juniper Networks router. In each system log message directed to the remote machine, the hostname of the local Routing Engine appears after the timestamp to indicate that it is the source for the message.

To direct system log messages to the other Routing Engine on a router with two Routing Engines installed and operational, include the **host other-routing-engine** statement. The statement is not automatically reciprocal, so you must include it in each Routing Engine configuration if you want the Routing Engines to direct messages to each other. In each message directed to the other Routing Engine, the string **re0** or **re1** appears after the timestamp to indicate the source for the message.

For the list of logging facilities and severity levels to configure under the **host** statement, see *Specifying the Facility and Severity of Messages to Include in the Log*.

To record facility and severity level information in each message, include the **explicit-priority** statement. For more information, see "Including Priority Information in System Log Messages" on page 21.

For information about the **match** statement, see "Using Regular Expressions to Refine the Set of Logged Messages" on page 25.

When directing messages to remote machines, you can include the **source-address** statement to specify the IP address of the router that is reported in the messages as their source. In each **host** statement, include the **facility-override** statement to assign an alternative facility and the **log-prefix** statement to add a string to each message. You can include the **structured-data** statement to enable the forwarding of structured system log messages to a remote system log server in the IETF system log message format.

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 13

Specifying an Alternative Source Address for System Log Messages Directed to a Remote Destination

To specify the source router to be reported in system log messages when the messages are directed to a remote machine, include the **source-address** statement at the **[edit system syslog]** hierarchy level:

```
[edit system syslog]
source-address source-address;
```

source-address is a valid IPv4 or IPv6 address configured on one of the router interfaces. The address is reported in the messages directed to all remote machines specified in **host *hostname*** statements at the **[edit system syslog]** hierarchy level, but not in messages directed to the other Routing Engine.

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 13

- Examples: Assigning an Alternative Facility to System Log Messages Directed to a Remote Destination on page 37

Adding a Text String to System Log Messages Directed to a Remote Destination

To add a text string to every system log message directed to a remote machine or to the other Routing Engine, include the **log-prefix** statement at the **[edit system syslog host]** hierarchy level:

```
[edit system syslog host (hostname | other-routing-engine)]
facility severity;
log-prefix string;
```

The string can contain any alphanumeric or special character except the equal sign (=) and the colon (:). It also cannot include the space character; do not enclose the string in quotation marks (“ ”) in an attempt to include spaces in it.

The Junos OS system logging utility automatically appends a colon and a space to the specified string when the system log messages are written to the log. The string is inserted after the identifier for the Routing Engine that generated the message.

The following example shows how to add the string M120 to all messages to indicate that the router is an M120 router, and direct the messages to the remote machine hardware-logger.mycompany.com:

```
[edit system syslog]
host hardware-logger.mycompany.com {
  any info;
  log-prefix M120;
}
```

When these configuration statements are included on an M120 router called origin1, a message in the system log on hardware-logger.mycompany.com looks like the following:

```
Mar 9 17:33:23 origin1 M120: mgd[477]: UI_CMDLINE_READ_LINE: user ‘root’, command ‘run
  show version’
```

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 13
- Specifying Log File Size, Number, and Archiving Properties on page 19

Changing the Alternative Facility Name for System Log Messages Directed to a Remote Destination

Some facilities assigned to messages logged on the local router or switch have Junos OS-specific names (see Table 3 on page 5). In the recommended configuration, a remote machine designated at the **[edit system syslog host *hostname*]** hierarchy level is not a Juniper Networks router or switch, so its syslogd utility cannot interpret the Junos OS-specific names. To enable the standard syslogd utility to handle messages from these facilities when messages are directed to a remote machine, a standard **local*X*** facility name is used instead of the Junos OS-specific facility name.

Table 13 on page 35 lists the default alternative facility name next to the Junos OS-specific facility name it is used for.

The syslogd utility on a remote machine handles all messages that belong to a facility in the same way, regardless of the source of the message (the Juniper Networks router or switch or the remote machine itself). For example, the following statements in the configuration of the router called **local-router** direct messages from the **authorization** facility to the remote machine *monitor.mycompany.com*:

```
[edit system syslog]
host monitor.mycompany.com {
  authorization info;
}
```

The default alternative facility for the local **authorization** facility is also **authorization**. If the syslogd utility on **monitor** is configured to write messages belonging to the **authorization** facility to the file **/var/log/auth-attempts**, then the file contains the messages generated when users log in to **local-router** and the messages generated when users log in to **monitor**. Although the name of the source machine appears in each system log message, the mixing of messages from multiple machines can make it more difficult to analyze the contents of the **auth-attempts** file.

To make it easier to separate the messages from each source, you can assign an alternative facility to all messages generated on **local-router** when they are directed to **monitor**. You can then configure the syslogd utility on **monitor** to write messages with the alternative facility to a different file from messages generated on **monitor** itself.

To change the facility used for all messages directed to a remote machine, include the **facility-override** statement at the **[edit system syslog host *hostname*]** hierarchy level:

```
[edit system syslog host hostname]
facility severity;
facility-override facility;
```

In general, it makes sense to specify an alternative facility that is not already in use on the remote machine, such as one of the **local*X*** facilities. On the remote machine, you must also configure the syslogd utility to handle the messages in the desired manner.

Table 14 on page 36 lists the facilities that you can specify in the **facility-override** statement.

We do not recommend including the **facility-override** statement at the **[edit system syslog host other-routing-engine]** hierarchy level. It is not necessary to use alternative facility names when directing messages to the other Routing Engine, because its Junos OS system logging utility can interpret the Junos OS-specific names.

The following example shows how to log all messages generated on the local router at the error level or higher to the local0 facility on the remote machine called monitor.mycompany.com:

```
[edit system syslog]
host monitor.mycompany.com {
  any error;
  facility-override local0;
}
```

The following example shows how to configure routers located in California and routers located in New York to send messages to a single remote machine called central-logger.mycompany.com. The messages from California are assigned to alternative facility local0 and the messages from New York are assigned to alternative facility local2.

- Configure California routers to aggregate messages in the local0 facility:

  ```
  [edit system syslog]
  host central-logger.mycompany.com {
     change-log info;
     facility-override local0;
  }
  ```

- Configure New York routers to aggregate messages in the local2 facility:

  ```
  [edit system syslog]
  host central-logger.mycompany.com {
     change-log info;
     facility-override local2;
  }
  ```

On central-logger, you can then configure the system logging utility to write messages from the local0 facility to the file **change-log** and the messages from the local2 facility to the file **new-york-config**.

Related Documentation

- Table 13 on page 35
- Alternate Facilities for System Log Messages Directed to a Remote Destination on page 36
- Examples: Assigning an Alternative Facility to System Log Messages Directed to a Remote Destination on page 37

Default Facilities for System Log Messages Directed to a Remote Destination

Table 13 on page 35 lists the default alternative facility name next to the Junos OS-specific facility name for which it is used. For facilities that are not listed, the default alternative name is the same as the local facility name.

Table 13: Default Facilities for Messages Directed to a Remote Destination

Junos OS–Specific Local Facility	Default Facility When Directed to Remote Destination
change-log	local6
conflict-log	local5
dfc	local1
firewall	local3

Table 13: Default Facilities for Messages Directed to a Remote Destination *(continued)*

Junos OS–Specific Local Facility	Default Facility When Directed to Remote Destination
interactive-commands	local7
pfe	local4

Related Documentation

- Single-Chassis System Logging Configuration Overview on page 13

Alternate Facilities for System Log Messages Directed to a Remote Destination

Table 14 on page 36 lists the facilities that you can specify in the **facility-override** statement.

Table 14: Facilities for the facility-override Statement

Facility	Description
authorization	Authentication and authorization attempts
daemon	Actions performed or errors encountered by system processes
ftp	Actions performed or errors encountered by the FTP process
kernel	Actions performed or errors encountered by the Junos OS kernel
local0	Local facility number 0
local1	Local facility number 1
local2	Local facility number 2
local3	Local facility number 3
local4	Local facility number 4
local5	Local facility number 5
local6	Local facility number 6
local7	Local facility number 7
user	Actions performed or errors encountered by user-space processes

We do not recommend including the **facility-override** statement at the **[edit system syslog host other-routing-engine]** hierarchy level. It is not necessary to use alternative facility names when directing messages to the other Routing Engine, because its Junos OS system logging utility can interpret the Junos OS-specific names.

Related Documentation

- Examples: Assigning an Alternative Facility to System Log Messages Directed to a Remote Destination on page 37
- Single-Chassis System Logging Configuration Overview on page 13

Examples: Assigning an Alternative Facility to System Log Messages Directed to a Remote Destination

Log all messages generated on the local routing platform at the error level or higher to the **local0** facility on the remote machine called **monitor.mycompany.com**:

```
[edit system syslog]
host monitor.mycompany.com {
 any error;
 facility-override local0;
}
```

Configure routing platforms located in California and routing platforms located in New York to send messages to a single remote machine called central-logger.mycompany.com. The messages from California are assigned alternative facility local0 and the messages from New York are assigned to alternative facility local2.

- Configure California routing platforms to aggregate messages in the **local0** facility:

  ```
  [edit system syslog]
  host central-logger.mycompany.com {
   change-log info;
   facility-override local0;
  }
  ```

- Configure New York routing platforms to aggregate messages in the **local2** facility:

  ```
  [edit system syslog]
  host central-logger.mycompany.com {
   change-log info;
   facility-override local2;
  }
  ```

On **central-logger,** you can then configure the system logging utility to write messages from the **local0** facility to the file **california-config** and the messages from the **local2** facility to the file **new-york-config**.

Related Documentation

- Alternate Facilities for System Log Messages Directed to a Remote Destination on page 36

CHAPTER 4

Configuring System Logging for a TX Matrix Router

Configuring System Logging for a TX Matrix Router

To configure system logging for all routers in a routing matrix composed of a TX Matrix router and T640 routers, include the **syslog** statement at the **[edit system]** hierarchy level on the TX Matrix router. The **syslog** statement applies to every router in the routing matrix.

```
[edit system]
syslog {
  archive <files number> <size size <world-readable | no-world-readable>;
  console {
    facility severity;
  }
  file filename {
    facility severity;
    archive <archive-sites {ftp-url <password password>}> <files number> <size size>
      <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
      no-world-readable>;
    explicit-priority;
    match "regular-expression";
    structured-data {
      brief;
    }
  }
  host (hostname | other-routing-engine | scc-master) {
    facility severity;
```

```
        explicit-priority;
        facility-override facility;
        log-prefix string;
        match "regular-expression";
        source-address source-address;
        port port number;
      }
      source-address source-address;
      time-format (year | millisecond | year millisecond);
      (username | *) {
        facility severity;
        match "regular-expression";
      }
    }
```

When included in the configuration on the TX Matrix router, the following configuration statements have the same effect as on a single-chassis system, except that they apply to every router in the routing matrix:

- **archive**—Sets the size and number of log files on each platform in the routing matrix. See "Specifying Log File Size, Number, and Archiving Properties" on page 19.
- **console**—Directs the specified messages to the console of each platform in the routing matrix. See "Directing System Log Messages to the Console" on page 19.
- **file**—Directs the specified messages to a file of the same name on each platform in the routing matrix. See "Directing System Log Messages to a Log File" on page 17.
- **match**—Limits the set of messages logged to a destination to those that contain (or do not contain) a text string matching a regular expression. See "Using Regular Expressions to Refine the Set of Logged Messages" on page 25.

  The separate **match** statement at the **[edit system syslog host scc-master]** hierarchy level applies to messages forwarded from the T640 routers to the TX Matrix router. See "Configuring Optional Features for Forwarded Messages on a TX Matrix Router" on page 44.
- **port**—Specifies the port number of the remote syslog server.
- **source-address**—Sets the IP address of the router to report in system log messages as the message source, when the messages are directed to the remote machines specified in all **host *hostname*** statements at the **[edit system syslog]** hierarchy level, for each platform in the routing matrix. On a routing matrix composed of a TX Matrix router and T640 routers, the address is not reported by the T640 routers in messages directed to the other Routing Engine on each router or to the TX Matrix router. See "Specifying an Alternative Source Address for System Log Messages Directed to a Remote Destination" on page 32.
- **structured-data**—Writes messages to a file in structured-data format. See "Logging Messages in Structured-Data Format" on page 18.

- **time-format**—Adds the millisecond, year, or both to the timestamp in each standard-format message. See "Including the Year or Millisecond in Timestamps" on page 24.
- **user**—Directs the specified messages to the terminal session of one or more specified users on each platform in the routing matrix that they are logged in to. See "Directing System Log Messages to a User Terminal" on page 18.

The effect of the other statements differs somewhat for a routing matrix than for a single-chassis system.

Related Documentation

- Configuring Message Forwarding to the TX Matrix Router on page 41
- Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Router on page 42
- Configuring Optional Features for Forwarded Messages on a TX Matrix Router on page 44
- Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router on page 46
- Configuring System Logging Differently on Each T640 Router in a Routing Matrix on page 47

Configuring Message Forwarding to the TX Matrix Router

By default, the master Routing Engine on each T640 router forwards to the master Routing Engine on the TX Matrix router all messages from all facilities with severity level of **info** and higher. To change the facility, the severity level, or both, include the **host scc-master** statement at the **[edit system syslog]** hierarchy level on the TX Matrix router:

```
[edit system syslog]
host scc-master {
  facility severity;
}
```

To disable message forwarding, set the facility to **any** and the severity level to **none**:

```
[edit system syslog]
host scc-master {
  any none;
}
```

In either case, the setting applies to all T640 routers in the routing matrix.

To capture the messages forwarded by the T640 routers (as well as messages generated on the TX Matrix router itself), you must also configure system logging on the TX Matrix router. Direct the messages to one or more destinations by including the appropriate statements at the **[edit system syslog]** hierarchy level on the TX Matrix router:

- To a file, as described in "Directing System Log Messages to a Log File" on page 17.
- To the terminal session of one or more specific users (or all users), as described in "Directing System Log Messages to a User Terminal" on page 18.
- To the console, as described in "Directing System Log Messages to the Console" on page 19.
- To a remote machine that is running the syslogd utility or to the other Routing Engine. For more information, see "Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router" on page 46.

As previously noted, the configuration statements included on the TX Matrix router also configure the same destinations on each T640 router in the routing matrix.

When specifying the severity level for local messages (at the **[edit system syslog (file | host | console | user)]** hierarchy level) and forwarded messages (at the **[edit system syslog host scc-master]** hierarchy level), you can set the same severity level for both, set a lower severity level for local messages, or set a higher severity level for local messages. The following examples describe the consequence of each configuration. (For simplicity, the examples use the **any** facility in every case. You can also specify different severities for different facilities, with more complex consequences.)

Related Documentation

- Configuring System Logging for a TX Matrix Router on page 39

Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Router

This topic describes the impact of different local and forwarded severity levels configured for system log messages on a TX Matrix router:

Messages Logged When the Local and Forwarded Severity Levels Are the Same

When the severity level is the same for local and forwarded messages, the log on the TX Matrix router contains all messages from the logs on the T640 routers. For example, you can specify severity **info** for the **/var/log/messages** file, which is the default severity level for messages forwarded by T640 routers:

```
[edit system syslog]
file messages {
  any info;
}
```

Table 15 on page 43 specifies which messages are included in the logs on the T640 routers and the TX Matrix router.

Table 15: Example: Local and Forwarded Severity Level Are Both info

Log Location	Source of Messages	Lowest Severity Included
T640 router	Local	**info**
TX Matrix router	Local	**info**
	Forwarded from T640 routers	**info**

Messages Logged When the Local Severity Level Is Lower

When the severity level is lower for local messages than for forwarded messages, the log on the TX Matrix router includes fewer forwarded messages than when the severities are the same. Locally generated messages are still logged at the lower severity level, so their number in each log is the same as when the severities are the same.

For example, on a TX Matrix router, you can specify severity **notice** for the **/var/log/messages** file and severity **critical** for forwarded messages:

```
[edit system syslog]
file messages {
    any notice;
}
host scc-master {
    any critical;
}
```

Table 16 on page 43 specifies which messages in a routing matrix are included in the logs on the T640 routers and the TX Matrix router. The T640 routers forward only those messages with severity **critical** and higher, so the log on the TX Matrix router does not include the messages with severity **error**, **warning**, or **notice** that the T640 routers log locally.

Table 16: Example: Local Severity Is notice, Forwarded Severity Is critical

Log Location	Source of Messages	Lowest Severity Included
T640 router	Local	**notice**
TX Matrix router	Local	**notice**
	Forwarded from T640 routers	**critical**

Messages Logged When the Local Severity Level Is Higher

When the severity level is higher for local messages than for forwarded messages, the log on the TX Matrix router includes fewer forwarded messages than when the severities are the same, and all local logs contain fewer messages overall.

For example, you can specify severity **critical** for the **/var/log/messages** file and severity **notice** for forwarded messages:

```
[edit system syslog]
file messages {
   any critical;
}
host scc-master {
   any notice;
}
```

Table 17 on page 44 specifies which messages are included in the logs on the T640 routers and the TX Matrix router. Although the T640 routers forward messages with severity **notice** and higher, the TX Matrix router discards any of those messages with severity lower than **critical** (does not log forwarded messages with severity **error**, **warning**, or **notice**). None of the logs include messages with severity **error** or lower.

Table 17: Example: Local Severity Is critical, Forwarded Severity Is notice

Log Location	Source of Messages	Lowest Severity Included
T640 router	Local	**critical**
TX Matrix router	Local	**critical**
	Forwarded from T640 routers	**critical**

Related Documentation

- Configuring System Logging for a TX Matrix Router on page 39

Configuring Optional Features for Forwarded Messages on a TX Matrix Router

To configure additional optional features when specifying how the T640 routers forward messages to the TX Matrix router, include statements at the **[edit system syslog host scc-master]** hierarchy level. To include priority information (facility and severity level) in each forwarded message, include the **explicit-priority** statement. To insert a text string in each forwarded message, include the **log-prefix** statement. To use regular expression matching to specify more exactly which messages from a facility are forwarded, include the **match** statement.

```
[edit system syslog]
host scc-master {
   facility severity;
   explicit-priority;
   log-prefix string;
   match "regular-expression";
}
```

You can also include the **facility-override** statement at the **[edit system syslog host scc-master]** hierarchy level, but we do not recommend doing so. It is not necessary to use alternative facilities for messages forwarded to the TX Matrix router, because it runs the Junos system logging utility and can interpret the Junos OS-specific facilities. For more information about alternative facilities, see "Changing the Alternative Facility Name for System Log Messages Directed to a Remote Destination" on page 33.

- Including Priority Information in Forwarded Messages on page 45
- Adding a Text String to Forwarded Messages on page 45
- Using Regular Expressions to Refine the Set of Forwarded Messages on page 46

Including Priority Information in Forwarded Messages

When you include the **explicit-priority** statement at the **[edit system syslog host scc-master]** hierarchy level, messages forwarded to the TX Matrix router include priority information. For the information to appear in a log file on the TX Matrix router, you must also include the **explicit-priority** statement at the **[edit system syslog file *filename*]** hierarchy level for the file on the TX Matrix router. As a consequence, the log file with the same name on each platform in the routing matrix also includes priority information for locally generated messages.

To include priority information in messages directed to a remote machine from all routers in the routing matrix, also include the **explicit-priority** statement at the **[edit system syslog host *hostname*]** hierarchy level for the remote machine. For more information, see "Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router" on page 46.

In the following example, the **/var/log/messages** file on all routers includes priority information for messages with severity **notice** and higher from all facilities. The log on the TX Matrix router also includes messages with those characteristics forwarded from the T640 routers.

```
[edit system syslog]
host scc-master {
   any notice;
   explicit-priority;
}
file messages {
   any notice;
   explicit-priority;
}
```

Adding a Text String to Forwarded Messages

When you include the **log-prefix** statement at the **[edit system syslog host scc-master]** hierarchy level, the string that you define appears in every message forwarded to the TX Matrix router. For more information, see "Adding a Text String to System Log Messages Directed to a Remote Destination" on page 33.

Using Regular Expressions to Refine the Set of Forwarded Messages

When you include the **match** statement at the **[edit system syslog host scc-master]** hierarchy level, the regular expression that you specify controls which messages from the T640 routers are forwarded to the TX Matrix router. The regular expression is not applied to messages from the T640 router that are directed to destinations other than the TX Matrix router. For more information about regular expression matching, see "Using Regular Expressions to Refine the Set of Logged Messages" on page 25.

Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router

You can configure a routing matrix composed of a TX Matrix router and T640 routers to direct system logging messages to a remote machine or the other Routing Engine on each router, just as on a single-chassis system. Include the **host** statement at the **[edit system syslog]** hierarchy level on the TX Matrix router:

```
[edit system syslog]
host (hostname | other-routing-engine) {
   facility severity;
   explicit-priority;
   facility-override facility;
   log-prefix string;
   match "regular-expression";
}
source-address source-address;
```

The TX Matrix router directs messages to a remote machine or the other Routing Engine in the same way as a single-chassis system, and the optional statements (**explicit-priority**, **facility-override**, **log-prefix**, **match**, and **source-address**) also have the same effect as on a single-chassis system. For more information, see "Directing System Log Messages to a Remote Machine or the Other Routing Engine" on page 31.

For the TX Matrix router to include priority information when it directs messages that originated on a T640 router to the remote destination, you must also include the **explicit-priority** statement at the **[edit system syslog host scc-master]** hierarchy level.

The **other-routing-engine** statement does not interact with message forwarding from the T640 routers to the TX Matrix router. For example, if you include the statement in the configuration for the Routing Engine in slot 0 (**re0**), the **re0** Routing Engine on each T640 router sends messages to the **re1** Routing Engine on its platform only. It does not also send messages directly to the **re1** Routing Engine on the TX Matrix router.

Because the configuration on the TX Matrix router applies to the T640 routers, any T640 router that has interfaces for direct access to the Internet also directs messages to the remote machine. The consequences include the following:

- If the T640 routers are configured to forward messages to the TX Matrix router (as in the default configuration), the remote machine receives two copies of some messages: one directly from the T640 router and the other from the TX Matrix router. Which messages are duplicated depends on whether the severities are the same for local logging and for forwarded messages. For more information, see "Configuring Message Forwarding to the TX Matrix Router" on page 41.

- If the **source-address** statement is configured at the **[edit system syslog]** hierarchy level, all routers in the routing matrix report the same source address in messages directed to the remote machine. This is appropriate, because the routing matrix functions as a single router.
- If the **log-prefix** statement is included, the messages from all routers in the routing matrix include the same text string. You cannot use the string to distinguish between the routers in the routing matrix.

Related Documentation

- Configuring System Logging for a TX Matrix Router on page 39

Configuring System Logging Differently on Each T640 Router in a Routing Matrix

We recommend that all routers in a routing matrix composed of a TX Matrix router and T640 routers use the same configuration, which implies that you include system logging configuration statements on the TX Matrix router only. In rare circumstances, however, you might choose to log different messages on different routers. For example, if one router in the routing matrix is experiencing problems with authentication, a Juniper Networks support representative might instruct you to log messages from the **authorization** facility with severity **debug** on that router.

To configure routers separately, include configuration statements in the appropriate groups at the **[edit groups]** hierarchy level on the TX Matrix router:

- To configure settings that apply to the TX Matrix router but not the T640 routers, include them in the **re0** and **re1** configuration groups.
- To configure settings that apply to particular T640 routers, include them in the **lcc*n*-re0** and **lcc*n*-re1** configuration groups, where ***n*** is the line-card chassis (LCC) index number of the router.

When you use configuration groups, do not issue CLI configuration-mode commands to change statements at the **[edit system syslog]** hierarchy level on the TX Matrix router. If you do, the resulting statements overwrite the statements defined in configuration groups and apply to the T640 routers also. (We further recommend that you do not issue CLI configuration-mode commands on the T640 routers at any time.)

The following example shows how to configure the **/var/log/messages** files on three routers to include different sets of messages:

- On the TX Matrix router, local messages with severity **info** and higher from all facilities. The file does not include messages from the T640 routers, because the **host scc-master** statement disables message forwarding.
- On the T640 router designated **LCC0**, messages from the **authorization** facility with severity **info** and higher.
- On the T640 router designated **LCC1**, messages with severity **notice** from all facilities.

```
[edit groups]
re0 {
   system {
      syslog {
         file messages {
            any info;
         }
         host scc-master {
            any none;
         }
      }
   }
}
re1 {
   ... same statements as for re0 ...
}
lcc0-re0 {
   system {
      syslog {
         file messages {
            authorization info;
         }
      }
   }
}
lcc0-re1 {
   ... same statements as for lcc0-re0 ...
}
lcc1-re0 {
   system {
      syslog {
         file messages {
            any notice;
         }
      }
   }
}
lcc0-re1 {
   ... same statements as for lcc1-re0 ...
}
```

Related Documentation

- Configuring System Logging for a TX Matrix Router on page 39

CHAPTER 5

Configuring System Logging for a TX Matrix Plus Router

Configuring System Logging for a TX Matrix Plus Router

From the perspective of the user interface, the routing matrix appears as a single router. The TX Matrix Plus router (also called the switch-fabric chassis SFC) controls all the T1600 or T4000 routers (also called the line-card chassis LCC) in the routing matrix.

To configure system logging for all routers in a routing matrix composed of a TX Matrix Plus router with connected T1600 or T4000 LCCs, include the **syslog** statement at the **[edit system]** hierarchy level on the SFC. The **syslog** statement applies to every router in the routing matrix.

```
[edit system]
syslog {
  archive <files number> <size size <world-readable | no-world-readable>;
  console {
    facility severity;
  }
  file filename {
    facility severity;
    archive <archive-sites {ftp-url <password password>}> <files number> <size size>
      <start-time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable |
      no-world-readable>;
    explicit-priority;
```

```
            match "regular-expression";
            structured-data {
               brief;
            }
         }
         host (hostname | other-routing-engine | sfc0-master) {
            facility severity;
            explicit-priority;
            facility-override facility;
            log-prefix string;
            match "regular-expression";
         }
         source-address source-address;
         time-format (year | millisecond | year millisecond);
         (username | *) {
            facility severity;
            match "regular-expression";
         }
      }
```

When included in the configuration on the TX Matrix Plus router, the following configuration statements have the same effect as on a single-chassis system, except that they apply to every router in the routing matrix.

- **archive**—Sets the size and number of log files on each router in the routing matrix. See "Specifying Log File Size, Number, and Archiving Properties" on page 19.
- **console**—Directs the specified messages to the console of each router in the routing matrix. See "Directing System Log Messages to the Console" on page 19.
- **file**—Directs the specified messages to a file of the same name on each router in the routing matrix. See "Directing System Log Messages to a Log File" on page 17.
- **match**—Limits the set of messages logged to a destination to those that contain (or do not contain) a text string matching a regular expression. See "Using Regular Expressions to Refine the Set of Logged Messages" on page 25.

  The separate **match** statement at the **[edit system syslog host sfc0-master]** hierarchy level applies to messages forwarded from the T1600 or T4000 LCCs to the SFC. See "Configuring Optional Features for Forwarded Messages on a TX Matrix Plus Router" on page 54.
- **source-address**—Sets the IP address of the router as the message source in system log messages when the messages are directed to the remote machines specified in all **host *hostname*** statements at the **[edit system syslog]** hierarchy level, for each router in the routing matrix. On a routing matrix composed of a TX Matrix Plus router with connected T1600 or T4000 LCCs, the address is not reported by the T1600 or T4000 routers in messages directed to the other Routing Engine on each router or to the TX Matrix Plus router. See "Specifying an Alternative Source Address for System Log Messages Directed to a Remote Destination" on page 32.
- **structured-data**—Writes messages to a file in structured-data format. See "Logging Messages in Structured-Data Format" on page 18.

- **time-format**—Adds the millisecond, year, or both to the timestamp in each standard-format message. See "Including the Year or Millisecond in Timestamps" on page 24.
- **user**—Directs the specified messages to the terminal session of one or more specified users on each router in the routing matrix that they are logged in to. See "Directing System Log Messages to a User Terminal" on page 18.

The effect of the other statements differs somewhat for a routing matrix than for a single-chassis system.

Related Documentation

- Configuring Message Forwarding to the TX Matrix Plus Router on page 51
- Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Plus Router on page 52
- Configuring Optional Features for Forwarded Messages on a TX Matrix Plus Router on page 54
- Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router on page 56
- Configuring System Logging Differently on Each T1600 or T4000 Router in a Routing Matrix on page 57
- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

Configuring Message Forwarding to the TX Matrix Plus Router

From the perspective of the user interface, the routing matrix appears as a single router. The TX Matrix Plus router (also called the switch-fabric chassis SFC) controls all the T1600 or T4000 routers (also called the line-card chassis LCC) in the routing matrix.

By default, the master Routing Engine on each connected T1600 or T4000 LCC forwards to the master Routing Engine on the SFC all messages from all facilities with severity level of **info** and higher. To change the facility, the severity level, or both, include the **host sfc0-master** statement at the **[edit system syslog]** hierarchy level on the SFC:

```
[edit system syslog]
host sfc0-master {
   facility severity;
}
```

To disable message forwarding, set the facility to **any** and the severity level to **none**:

```
[edit system syslog]
host sfc0-master {
   any none;
}
```

In either case, the setting applies to all connected LCCs in the routing matrix.

To capture the messages forwarded by the T1600 or T4000 LCCs (as well as messages generated on the SFC itself), you must also configure system logging on the SFC. Direct the messages to one or more destinations by including the appropriate statements at the **[edit system syslog]** hierarchy level on the SFC:

- To a file, as described in "Directing System Log Messages to a Log File" on page 17.
- To the terminal session of one or more specific users (or all users), as described in "Directing System Log Messages to a User Terminal" on page 18.
- To the console, as described in "Directing System Log Messages to the Console" on page 19.
- To a remote machine that is running the syslogd utility or to the other Routing Engine. For more information, see "Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router" on page 56.

As previously noted, the configuration statements included on the SFC also configure the same destinations on each connected LCC.

When specifying the severity level for local messages (at the **[edit system syslog (file | host | console | user)]** hierarchy level) and forwarded messages (at the **[edit system syslog host sfc0-master]** hierarchy level), you can set the same severity level for both, set a lower severity level for local messages, or set a higher severity level for local messages. The following examples describe the consequence of each configuration. (For simplicity, the examples use the **any** facility in every case. You can also specify different severities for different facilities, with more complex consequences.)

Related Documentation

- Configuring System Logging for a TX Matrix Plus Router on page 49
- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Plus Router

This topic describes the impact of different local and forwarded severity levels configured for the system log messages on a TX Matrix Plus router:

- Messages Logged When the Local and Forwarded Severity Levels Are the Same on page 52
- Messages Logged When the Local Severity Level Is Lower on page 53
- Messages Logged When the Local Severity Level Is Higher on page 54

Messages Logged When the Local and Forwarded Severity Levels Are the Same

When the severity level is the same for local and forwarded messages, the log on the TX Matrix Plus router contains all messages from the logs on the T1600 routers in the routing matrix. For example, you can specify severity **info** for the **/var/log/messages** file, which is the default severity level for messages forwarded by T1600 routers:

```
[edit system syslog]
```

```
file messages {
   any info;
}
```

Table 18 on page 53 specifies which messages in a routing matrix based on a TX Matrix Plus router are included in the logs on the T1600 routers and the TX Matrix Plus router:

Table 18: Example: Local and Forwarded Severity Level Are Both info

Log Location	Source of Messages	Lowest Severity Included
T1600 router	Local	**info**
TX Matrix Plus router	Local	**info**
	Forwarded from T1600 routers	**info**

Messages Logged When the Local Severity Level Is Lower

When the severity level is lower for local messages than for forwarded messages, the log on the TX Matrix Plus router includes fewer forwarded messages than when the severities are the same. Locally generated messages are still logged at the lower severity level, so their number in each log is the same as when the severities are the same.

For example, on a TX Matrix Plus router, you can specify severity **notice** for the **/var/log/messages** file and severity **critical** for forwarded messages:

```
[edit system syslog]
file messages {
   any notice;
}
host sfc0-master {
   any critical;
}
```

Table 19 on page 53 specifies which messages in a routing matrix are included in the logs on the T1600 routers and the TX Matrix Plus router. The T1600 routers forward only those messages with severity **critical** and higher, so the log on the TX Matrix Plus router does not include the messages with severity **error**, **warning**, or **notice** that the T1600 routers log locally.

Table 19: Example: Local Severity Is notice, Forwarded Severity Is critical

Log Location	Source of Messages	Lowest Severity Included
T1600 router	Local	**notice**
TX Matrix Plus router	Local	**notice**
	Forwarded from T1600 routers	**critical**

Messages Logged When the Local Severity Level Is Higher

When the severity level is higher for local messages than for forwarded messages, the log on the TX Matrix Plus router includes fewer forwarded messages than when the severities are the same, and all local logs contain fewer messages overall.

For example, you can specify severity **critical** for the **/var/log/messages** file and severity **notice** for forwarded messages:

```
[edit system syslog]
file messages {
   any critical;
}
host sfc0-master {
   any notice;
}
```

Table 20 on page 54 specifies which messages are included in the logs on the T1600 routers and the TX Matrix Plus router. Although the T1600 routers forward messages with severity **notice** and higher, the TX Matrix Plus router discards any of those messages with severity lower than **critical** (does not log forwarded messages with severity **error**, **warning**, or **notice**). None of the logs include messages with severity **error** or lower.

Table 20: Example: Local Severity Is critical, Forwarded Severity Is notice

Log Location	Source of Messages	Lowest Severity Included
T1600 router	Local	**critical**
TX Matrix Plus router	Local	**critical**
	Forwarded from T1600 routers	**critical**

Related Documentation

- Configuring System Logging for a TX Matrix Plus Router on page 49

Configuring Optional Features for Forwarded Messages on a TX Matrix Plus Router

From the perspective of the user interface, the routing matrix appears as a single router. The TX Matrix Plus router (also called the switch-fabric chassis SFC) controls all the T1600 or T4000 routers (also called the line-card chassis LCC) in the routing matrix.

To configure additional optional features when specifying how the connected T1600 or T4000 LCCs forward messages to the SFC, include statements at the **[edit system syslog host sfc0-master]** hierarchy level. To include priority information (facility and severity level) in each forwarded message, include the **explicit-priority** statement. To insert a text string in each forwarded message, include the **log-prefix** statement. To use regular expression matching to specify more exactly which messages from a facility are forwarded, include the **match** statement.

```
[edit system syslog]
```

```
host sfc0-master {
    facility severity;
    explicit-priority;
    log-prefix string;
    match "regular-expression;
}
```

You can also include the **facility-override** statement at the **[edit system syslog host sfc0-master]** hierarchy level, but we do not recommend doing so. It is not necessary to use alternative facilities for messages forwarded to the SFC, because it runs the Junos system logging utility and can interpret the Junos OS-specific facilities. For more information about alternative facilities, see "Changing the Alternative Facility Name for System Log Messages Directed to a Remote Destination" on page 33.

1. Including Priority Information in Forwarded Messages on page 55
2. Adding a Text String to Forwarded Messages on page 55
3. Using Regular Expressions to Refine the Set of Forwarded Messages on page 56

Including Priority Information in Forwarded Messages

When you include the **explicit-priority** statement at the **[edit system syslog host sfc0-master]** hierarchy level, messages forwarded to the TX Matrix Plus router (or the SFC) include priority information. For the information to appear in a log file on the SFC, you must also include the **explicit-priority** statement at the **[edit system syslog file *filename*]** hierarchy level for the file on the SFC. As a consequence, the log file with the same name on each platform in the routing matrix also includes priority information for locally generated messages.

To include priority information in messages directed to a remote machine from all routers in the routing matrix, also include the **explicit-priority** statement at the **[edit system syslog host *hostname*]** hierarchy level for the remote machine. For more information, see "Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router" on page 56.

In the following example, the **/var/log/messages** file on all routers includes priority information for messages with severity **notice** and higher from all facilities. The log on the TX Matrix Plus router SFC also includes messages with those characteristics forwarded from the connected T1600 or T4000 LCCs.

```
[edit system syslog]
host sfc0-master {
    any notice;
    explicit-priority;
}
file messages {
    any notice;
    explicit-priority;
}
```

Adding a Text String to Forwarded Messages

When you include the **log-prefix** statement at the **[edit system syslog host sfc0-master]** hierarchy level, the string that you define appears in every message forwarded to the TX

Matrix Plus router. For more information, see “Adding a Text String to System Log Messages Directed to a Remote Destination” on page 33.

Using Regular Expressions to Refine the Set of Forwarded Messages

When you include the **match** statement at the **[edit system syslog host sfc0-master]** hierarchy level, the regular expression that you specify controls which messages from the connected T1600 or T4000 LCCs are forwarded to the TX Matrix Plus SFC. The regular expression is not applied to messages from the connected LCCs that are directed to destinations other than the SFC. For more information about regular expression matching, see “Using Regular Expressions to Refine the Set of Logged Messages” on page 25.

Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router

From the perspective of the user interface, the routing matrix appears as a single router. The TX Matrix Plus router (also called the switch-fabric chassis SFC) controls all the T1600 or T4000 routers also called the ine-card chassis LCC) in the routing matrix.

You can configure a routing matrix composed of a TX Matrix Plus router with connected T1600 or T4000 LCCs to direct system logging messages to a remote machine or the other Routing Engine on each routing router, just as on a single-chassis system. Include the **host** statement at the **[edit system syslog]** hierarchy level on the SFC:

```
[edit system syslog]
host (hostname | other-routing-engine) {
  facility severity;
  explicit-priority;
  facility-override facility;
  log-prefix string;
  match "regular-expression";
}
source-address source-address;
```

The TX Matrix Plus router directs messages to a remote machine or the other Routing Engine in the same way as a single-chassis system, and the optional statements (**explicit-priority**, **facility-override**, **log-prefix**, **match**, and **source-address**) also have the same effect as on a single-chassis system. For more information, see “Directing System Log Messages to a Remote Machine or the Other Routing Engine” on page 31.

For the TX Matrix Plus router to include priority information when it directs messages that originated on a connected T1600 or T4000 LCC to the remote destination, you must also include the **explicit-priority** statement at the **[edit system syslog host sfc0-master]** hierarchy level.

The **other-routing-engine** statement does not interact with message forwarding from the connected T1600 or T4000 LCCs to the SFC. For example, if you include the statement in the configuration for the Routing Engine in slot 0 (**re0**), the **re0** Routing Engine on each connected T1600 or T4000 LCC sends messages to the **re1** Routing Engine on its router only. It does not also send messages directly to the **re1** Routing Engine on the SFC.

Because the configuration on the SFC applies to the connected T1600 or T4000 LCCs, any LCC that has interfaces for direct access to the Internet also directs messages to the remote machine. The consequences include the following:

- If the LCCs are configured to forward messages to the SFC (as in the default configuration), the remote machine receives two copies of some messages: one directly from the T1600 or T4000 LCC and the other from the SFC. Which messages are duplicated depends on whether the severities are the same for local logging and for forwarded messages. For more information, see “Configuring Message Forwarding to the TX Matrix Plus Router” on page 51.
- If the **source-address** statement is configured at the **[edit system syslog]** hierarchy level, all routers in the routing matrix report the same source address in messages directed to the remote machine. This is appropriate, because the routing matrix functions as a single routing router.
- If the **log-prefix** statement is included, the messages from all routers in the routing matrix include the same text string. You cannot use the string to distinguish between the routers in the routing matrix.

Related Documentation

- Configuring System Logging for a TX Matrix Plus Router on page 49
- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

Configuring System Logging Differently on Each T1600 or T4000 Router in a Routing Matrix

We recommend that all routers in a routing matrix composed of a TX Matrix Plus router with T1600 or T4000 routers use the same configuration, which implies that you include system logging configuration statements on the TX Matrix Plus router only. In rare circumstances, however, you might choose to log different messages on different routers. For example, if one router in the routing matrix is experiencing problems with authentication, a Juniper Networks support representative might instruct you to log messages from the **authorization** facility with severity **debug** on that router.

To configure routers separately, include configuration statements in the appropriate groups at the **[edit groups]** hierarchy level on the TX Matrix Plus router:

- To configure settings that apply to the TX Matrix Plus router but not the T1600 or T4000 routers, include them in the **re0** and **re1** configuration groups.
- To configure settings that apply to particular T1600 or T4000 routers, include them in the **lcc*n*-re0** and **lcc*n*-re1** configuration groups, where ***n*** is the line-card chassis (LCC) index number of the router.

When you use configuration groups, do not issue CLI configuration-mode commands to change statements at the **[edit system syslog]** hierarchy level on the TX Matrix Plus router. If you do, the resulting statements overwrite the statements defined in configuration groups and apply to the T1600 or T4000 routers also. (We further recommend that you do not issue CLI configuration-mode commands on the T1600 or T4000 routers at any time.)

For more information about the configuration groups for a routing matrix, see the chapter about configuration groups in the *CLI User Guide*.

The following example shows how to configure the **/var/log/messages** files on three routers to include different sets of messages:

- On the TX Matrix Plus router, local messages with severity **info** and higher from all facilities. The file does not include messages from the T1600 or T4000 routers, because the **host sfc0-master** statement disables message forwarding.
- On the T1600 or T4000 router designated **LCC0**, messages from the **authorization** facility with severity **info** and higher.
- On the T1600 or T4000 router designated **LCC1**, messages with severity **notice** from all facilities.

```
[edit groups]
re0 {
    system {
        syslog {
            file messages {
                any info;
            }
            host sfc0-master {
                any none;
            }
        }
    }
}
re1 {
    ... same statements as for re0 ...
}
lcc0-re0 {
    system {
        syslog {
            file messages {
                authorization info;
            }
        }
    }
}
lcc0-re1 {
    ... same statements as for lcc0-re0 ...
}
lcc1-re0 {
    system {
        syslog {
            file messages {
                any notice;
            }
        }
    }
}
```

```
lcc0-re1 {
   ... same statements as for lcc1-re0 ...
}
```

Related Documentation

- Configuring System Logging for a TX Matrix Plus Router on page 49
- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

Examples: Assigning an Alternative Facility

Log all messages generated on the local routing platform at the error level or higher to the **local0** facility on the remote machine called **monitor.mycompany.com**:

```
[edit system syslog]
host monitor.mycompany.com {
 any error;
 facility-override local0;
}
```

Configure routing platforms located in California and routing platforms located in New York to send messages to a single remote machine called **central-logger.mycompany.com.** The messages from California are assigned alternative facility **local0** and the messages from New York are assigned to alternative facility **local2**.

- Configure California routing platforms to aggregate messages in the **local0** facility:

  ```
  [edit system syslog]
  host central-logger.mycompany.com {
   change-log info;
   facility-override local0;
  }
  ```

- Configure New York routing platforms to aggregate messages in the **local2** facility:

  ```
  [edit system syslog]
  host central-logger.mycompany.com {
   change-log info;
   facility-override local2;
  }
  ```

On **central-logger,** you can then configure the system logging utility to write messages from the **local0** facility to the file **california-config** and the messages from the **local2** facility to the file **new-york-config**.

Related Documentation

- Alternate Facilities for System Log Messages Directed to a Remote Destination on page 36

CHAPTER 6

Displaying System Log Files

Displaying a Log File from a Single-Chassis System

To display a log file stored on a single-chassis system, enter Junos OS CLI operational mode and issue either of the following commands:

```
user@host> show loglog-filename
user@host> file show log-file-pathname
```

By default, the commands display the file stored on the local Routing Engine. To display the file stored on a particular Routing Engine, prefix the file or pathname with the string **re0** or **re1** and a colon. The following examples both display the **/var/log/messages** file stored on the Routing Engine in slot 1:

```
user@host> show log re1:messages
user@host> file show re1:/var/log/messages
```

For information about the fields in a log message, see “Interpreting Messages Generated in Standard Format by a Junos OS Process or Library” on page 67, “Interpreting Messages Generated in Standard Format by Services on a PIC” on page 71, and “Interpreting Messages Generated in Structured-Data Format” on page 72. For examples, see “Examples: Displaying a Log File” on page 61.

Examples: Displaying a Log File

Display the contents of the **/var/log/messages** file stored on the local Routing Engine. (The **/var/log** directory is the default location for log files, so you do not need to include it in the filename. The **messages** file is a commonly configured destination for system log messages.)

```
user@host> show log messages Apr 11 10:27:25 router1 mgd[3606]:
  UI_DBASE_LOGIN_EVENT: User 'barbara' entering configuration mode
Apr 11 10:32:22 router1 mgd[3606]: UI_DBASE_LOGOUT_EVENT: User 'barbara' exiting
  configuration mode
Apr 11 11:36:15 router1 mgd[3606]: UI_COMMIT: User 'root' performed commit: no comment
Apr 11 11:46:37 router1 mib2d[2905]: SNMP_TRAP_LINK_DOWN: ifIndex 82, ifAdminStatus
   up(1), ifOperStatus down(2), ifName at-1/0/0
```

Display the contents of the file **/var/log/processes**, which has been previously configured to include messages from the **daemon** facility. When issuing the **file show** command, you must specify the full pathname of the file:

```
user@host> file show /var/log/processes Feb 22 08:58:24 router1 snmpd[359]:
   SNMPD_TRAP_WARM_START: trap_generate_warm: SNMP trap: warm start
Feb 22 20:35:07 router1 snmpd[359]: SNMPD_THROTTLE_QUEUE_DRAINED:
   trap_throttle_timer_handler: cleared all throttled traps
Feb 23 07:34:56 router1 snmpd[359]: SNMPD_TRAP_WARM_START: trap_generate_warm:
   SNMP trap: warm start
Feb 23 07:38:19 router1 snmpd[359]: SNMPD_TRAP_COLD_START: trap_generate_cold:
   SNMP trap: cold start
```

Display the contents of the file **/var/log/processes** when the **explicit-priority** statement is included at the [**edit system syslog file processes**] hierarchy level:

```
user@host> file show /var/log/processes Feb 22 08:58:24 router1 snmpd[359]:
%DAEMON-3-SNMPD_TRAP_WARM_START: trap_generate_warm: SNMP trap: warm
   start
Feb 22 20:35:07 router1 snmpd[359]:
%DAEMON-6-SNMPD_THROTTLE_QUEUE_DRAINED: trap_throttle_timer_handler: cleared
   all throttled traps
Feb 23 07:34:56 router1 snmpd[359]:
%DAEMON-3-SNMPD_TRAP_WARM_START: trap_generate_warm: SNMP trap: warm
   start
Feb 23 07:38:19 router1 snmpd[359]:
%DAEMON-2-SNMPD_TRAP_COLD_START: trap_generate_cold: SNMP trap: cold start
```

Displaying a Log File from a Routing Matrix

One way to display a log file stored on the local Routing Engine of any of the individual platforms in a routing matrix (T640 routing nodes or TX Matrix platform) is to log in to a Routing Engine on the platform, enter Junos OS CLI operational mode, and issue the **show log** or **file show** command described in "Displaying a Log File from a Single-Chassis System" on page 61.

To display a log file stored on a T640 routing node during a terminal session on the TX Matrix platform, issue the **show log** or **file show** command and add a prefix that specifies the T640 routing node's LCC index number as lccn, followed by a colon. The index can be from 0 (zero) through 3:

```
user@host> show log lccn:log-filename
user@host> file show lccn:log-file-pathname
```

By default, the **show log** and **file show** commands display the specified log file stored on the master Routing Engine on the T640 routing node. To display the log from a particular Routing Engine, prefix the file- or pathname with the string lccn-master, **lccn-re0**, or **lccn-re1**, followed by a colon. The following examples all display the **/var/log/messages** file stored on the master Routing Engine (in slot 0) on routing node LCC2:

```
user@host> show log lcc2:messages
user@host> show log lcc2-master:messages
```

```
user@host> show log lcc2-re0:messages
user@host> file show lcc2:/var/log/messages
```

If the T640 routing nodes are forwarding messages to the TX Matrix platform (as in the default configuration), another way to view messages generated on a T640 routing node during a terminal session on the TX Matrix platform is simply to display a local log file. However, the messages are intermixed with messages from other T640 routing nodes and the TX Matrix platform itself. For more information about message forwarding, see "Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Router" on page 42.

For information about the fields in a log message, see "Interpreting Messages Generated in Structured-Data Format" on page 72, "Interpreting Messages Generated in Standard Format by Services on a PIC" on page 71, and "Interpreting Messages Generated in Standard Format by a Junos OS Process or Library" on page 67. For examples, see "Examples: Displaying a Log File" on page 61.

CHAPTER 7

Displaying and Interpreting System Log Message Descriptions

Displaying and Interpreting System Log Message Descriptions

This reference lists the messages available at the time of its publication. To display the list of messages that applies to the version of Junos OS that is running on a routing platform, enter the Junos OS CLI operational mode and issue the following command:

```
user@host> help syslog ?
```

To display the list of available descriptions for tags whose names begin with a specific character string, substitute the string (in all capital letters) for the variable ***TAG-PREFIX*** (there is no space between the prefix and the question mark):

```
user@host> help syslog TAG-PREFIX?
```

To display the complete descriptions for tags whose name includes a regular expression, substitute a Perl-based expression for the variable regex. The match is not case-sensitive. For information about Perl-based regular expressions, consult a Perl reference manual or website such as http://perldoc.perl.org.

```
user@host> help syslog regex
```

To display the complete description of a particular message, substitute its name for the variable ***TAG*** (in all capital letters):

```
user@host> help syslog TAG
```

Table 21 on page 66 describes the fields in a system log message description in this reference or in the CLI.

Table 21: Fields in System Log Message Descriptions

Field Name in Reference	Field Name in CLI	Description
—	**Name**	The message tag in all capital letters.
System Log Message	**Message**	Text of the message written to the system log. In the log, a specific value is substituted for each variable that appears in italics in this reference or in angle brackets (<>) in the CLI. In this reference, the message text appears on the second line of the **System Log Message** field. The first line is the message tag (the same text as in the **CLI** Name field). The prefix on each tag identifies the message source and the rest of the tag indicates the specific event or error.
—	**Help**	Short description of the message, which also appears in the right-hand column of CLI output for the **help syslog** command when the output lists multiple messages.
Description	**Description**	More detailed explanation of the message.
Type	**Type**	Category to which the message belongs: • **Error**: The message reports an error or failure condition that might require corrective action. • **Event**: The message reports a condition or occurrence that does not generally require corrective action.
Severity	**Severity**	Message severity level as described in Table: **System Log Message Severity Levels** in "Specifying the Facility and Severity of Messages to Include in the Log" on page 15.

Table 21: Fields in System Log Message Descriptions *(continued)*

Field Name in Reference	Field Name in CLI	Description
Cause	Cause	(Optional) Possible cause for message generation. There can be more than one cause.
Action	Action	(Optional) Action you can perform to resolve the error or failure condition described in the message. If this field does not appear in an entry, either no action is required or the action is self-explanatory.

Interpreting Messages Generated in Standard Format by a Junos OS Process or Library

The syntax of a standard-format message generated by a Junos OS process or subroutine library depends on whether it includes priority information:

- When the **explicit-priority** statement is included at the [**edit system syslog file *filename***] or [**edit system syslog host (*hostname* | other-routing-engine)**] hierarchy level, a system log message has the following syntax:

  ```
  timestamp  message-source: %facility-severity-TAG: message-text
  ```

- When directed to the console or to users, or when the **explicit-priority** statement is not included for files or remote hosts, a system log message has the following syntax:

  ```
  timestamp  message-source: TAG: message-text
  ```

Table 22 on page 67 describes the message fields.

Table 22: Fields in Standard-Format Messages Generated by a Junos OS process or Library

Field	Description
timestamp	Time at which the message was logged.
message-source	Identifier of the process or component that generated the message and the routing platform on which the message was logged. This field includes two or more subfields, depending on how system logging is configured. See “The message-source Field on a TX Matrix Platform” on page 68,“The message-source Field on a T640 Routing Node in a Routing Matrix” on page 70, and “The message-source Field on a Single-Chassis System” on page 68.
facility	Code that specifies the facility to which the system log message belongs. For a mapping of codes to facility names, see Table: *Numerical Codes for Severity Levels Reported in Priority Information* in “Including Priority Information in System Log Messages” on page 21.

Table 22: Fields in Standard-Format Messages Generated by a Junos OS process or Library *(continued)*

Field	Description
severity	Numerical code that represents the severity level assigned to the system log message. For a mapping of codes to severity names, see Table: *Numerical Codes for Severity Levels Reported in Priority Information* in "Including Priority Information in System Log Messages" on page 21.
TAG	Text string that uniquely identifies the message, in all uppercase letters and using the underscore (_) to separate words. The tag name begins with a prefix that indicates the generating software process or library. The entries in this reference are ordered alphabetically by this prefix. Not all processes on a routing platform use tags, so this field does not always appear.
message-text	Text of the message. For the text for each message, see the chapters following System Log Messages.

The message-source Field on a Single-Chassis System

The format of the ***message-source*** field in a message on a single-chassis system depends on whether the message was generated on the local Routing Engine or the other Routing Engine (on a system with two Routing Engines installed and operational). Messages from the other Routing Engine appear only if its configuration includes the **other-routing-engine** statement at the [**edit system syslog host**] hierarchy level.

- When the local Routing Engine generated the message, there are two subfields:

  ```
  hostname process[process-ID]
  ```

- When the other Routing Engine generated the message, there are three subfields:

  ```
  hostname reX process[process-ID]
  ```

hostname is the hostname of the local Routing Engine.

process[process-ID] is the name and PID of the process that generated the message. If the **re*X*** field also appears, the process is running on the other Routing Engine. If a process does not report its PID, the [*process-ID*] part does not appear.

re*X* indicates that the other Routing Engine generated the message (*X* is 0 or 1).

The message-source Field on a TX Matrix Platform

The format of the *message-source* field in a message on a TX Matrix platform depends on several factors:

- Whether the message was generated on the TX Matrix platform or a T640 routing node in the routing matrix. By default, the master Routing Engine on each T640 routing node forwards messages from all facilities with severity info and higher to the master

Routing Engine on the TX Matrix platform. When you configure system logging on the TX Matrix platform, its logs include the forwarded messages. For more information, see “Impact of Different Local and Forwarded Severity Levels on System Log Messages on a TX Matrix Router” on page 42.

- Whether the message was generated on the local Routing Engine or the other Routing Engine on the originating machine (TX Matrix platform or T640 routing node). Messages from the other Routing Engine appear only if its configuration includes the **other-routing-engine** statement at the [**edit system syslog host**] hierarchy level.
- Whether the message was generated by a kernel or user-space process, or by the microkernel on a hardware component.

Table 23 on page 69 specifies the format of the message-source field in the various cases.

Table 23: Format of message-source Field in Messages Logged on TX Matrix Platform

Generating Machine	Generating Routing Engine	Process or Component	Format
TX Matrix platform	Local	Process	***hostname process[processID]***
		Component	***hostname scc-reX process[processID]***
	Other	Process	***hostname scc-reX scc-componentZ process***
		Component	***hostname scc-reX scc-componentZ process***
T640 routing node	Local	Process	***hostname lccY-masterprocess[processID]***
		Component	***hostname lccY-master scc-componentZ process***
	Other	Process	***hostname lccY-master lccY-reX process[processID]***
		Component	***hostname lccY-master lccY-reX lccY-componentZ process***

hostname is the hostname of the local Routing Engine on the TX Matrix platform.

lccY*-master** is the master Routing Engine on the T640 routing node with the indicated LCC index number (Y*** is from 0 through 3).

lccY-reX indicates that the backup Routing Engine on the T640 routing node generated the message (***X*** is 0 or 1). The routing node has the indicated LCC index number (***Y*** matches the value in the **lccY-master** field.

lccY-componentZ process identifies the hardware component and process on the T640 routing node that generated the message (***Y*** matches the value in the **lccY-master** field and the range of values for ***Z*** depends on the component type). For example, **lcc2-fpc1 PFEMAN** refers to a process on the FPC in slot 1 on the T640 routing node with index LCC2.

process[process-ID] is the name and PID of the kernel or user-space process that generated the message. If the **scc-reX** or **lccY-reX** field also appears, the process is running on the other Routing Engine. If a process does not report its PID, the [***process-ID***] part does not appear.

scc-componentZ process identifies the hardware component and process on the TX Matrix platform that generated the message (the range of values for ***Z*** depends on the component type). For example, **spmb1 GSIB** refers to a process on one of the processor boards in the Switch Interface Board (SIB) with index 1.

scc-reX indicates that the other Routing Engine on the TX Matrix platform generated the message (***X*** is 0 or 1).

The message-source Field on a T640 Routing Node in a Routing Matrix

The format of the ***message-source*** field in a message on a T640 routing node in a routing matrix depends on two factors:

- Whether the message was generated on the local Routing Engine or the other Routing Engine. Messages from the other Routing Engine appear only if its configuration includes the **other-routing-engine** statement at the [**edit system syslog host**] hierarchy level.
- Whether the message was generated by a kernel or user-space process, or by the microkernel on a hardware component.

Table 24 on page 70 specifies the format of the ***message-source*** field in the various cases.

Table 24: Format of message-source Field in Messages Logged on TX Matrix Platform

Generating Routing Engine	Process or Component	Format
Local	Process	***hostname-lccY process[processID]***
	Component	***hostname-lccY lccY-componentZ process***
Other	Process	***hostname-lccY lccY-reX process[processID]***
	Component	***hostname-lccY lccY-reX lccY-componentZ process***

hostname-lccY is the hostname of the local Routing Engine and the T640 routing node's LCC index number.

lccY-componentZ process identifies the hardware component and process that generated the message (***Y*** matches the value in the ***hostname-lccY*** field and the range of values for ***Z*** depends on the component type). For example, lcc0-fpc0 CMLC refers to a process on the FPC in slot 0. The T640 routing node has index LCC0 in the routing matrix.

lccY-reX indicates that the other Routing Engine on the routing node generated the message (***Y*** matches the value in the ***hostname-lccY*** field and ***X*** is 0 or 1).

process[process-ID] is the name and PID of the kernel or user-space process that generated the message. If the ***lccY-reX*** field also appears, the process is running on the other Routing Engine. If a process does not report its PID, the [***process-ID***] part does not appear.

Interpreting Messages Generated in Standard Format by Services on a PIC

Standard-format system log messages generated by services on a PIC, such as the Adaptive Services (AS) PIC, have the following syntax:

```
timestamp  (FPC Slot fpc-slot, PIC Slot pic-slot) {service-set} [SERVICE]:
 optional-string TAG: message-text
```

NOTE: System logging for services on PICs is not configured at the [**edit system syslog**] hierarchy level as discussed in this chapter. For configuration information, see the *Junos Services Interfaces Configuration Guide*.

The (**FPC Slot** ***fpc-slot***, **PIC Slot** ***pic-slot***) field appears only when the standard system logging utility that runs on the Routing Engine writes the messages to the system log. When the PIC writes the message directly, the field does not appear.

Table 25 on page 71 describes the message fields.

Table 25: Fields in Messages Generated by a PIC

Field	Description
timestamp	Time at which the message was logged.
fpc-slot	Slot number of the Flexible PIC Concentrator (FPC) that houses the PIC that generated the message.
pic-slot	Number of the PIC slot on the FPC in which the PIC that generated the message resides.
service-set	Name of the service set that generated the message.
SERVICE	Code representing the service that generated the message. The codes include the following: • FWNAT—Network Address Translation (NAT) service • IDS—Intrusion detection service

Table 25: Fields in Messages Generated by a PIC *(continued)*

Field	Description
optional-string	A text string that appears if the configuration for the PIC includes the log-prefix statement at the [edit interfaces interface-name services-options syslog] hierarchy level. For more information, see the *Junos Services Interfaces Configuration Guide*.
TAG	Text string that uniquely identifies the message, in all uppercase letters and using the underscore (_) to separate words. The tag name begins with a prefix that indicates the generating PIC. The entries in this reference are ordered alphabetically by this prefix.
message-text	Text of the message. For the text of each message, see System Log Messages.

Interpreting Messages Generated in Structured-Data Format

Beginning in Junos OS Release 8.3, when the **structured-data** statement is included in the configuration for a log file, Junos OS processes and software libraries write messages to the file in structured-data format instead of the standard Junos OS format. For information about the **structured-data** statement, see "Logging Messages in Structured-Data Format" on page 18.

Structured-format makes it easier for automated applications to extract information from the message. In particular, the standardized format for reporting the value of variables (elements in the English-language message that vary depending on the circumstances that triggered the message) makes it easy for an application to extract those values. In standard format, the variables are interspersed in the message text and not identified as variables.

The structured-data format for a message includes the following fields (which appear here on two lines only for legibility):

<priority code>version timestamp hostname process processID TAG [junos@2636.platform variable-value-pairs] message-text

Table 26 on page 72 describes the fields. If the system logging utility cannot determine the value in a particular field, a hyphen (-) appears instead.

Table 26: Fields in Structured-Data Messages

Field	Description	Examples
<priority code>	Number that indicates the message's facility and severity. It is calculated by multiplying the facility number by 8 and then adding the numerical value of the severity. For a mapping of the numerical codes to facility and severity, see Table: **Facility and Severity Codes in the priority-code Field** in "Specifying the Facility and Severity of Messages to Include in the Log" on page 15.	<165> for a message from the **pfe** facility (facility=20) with severity **notice** (severity=5).

Table 26: Fields in Structured-Data Messages *(continued)*

Field	Description	Examples
version	Version of the Internet Engineering Task Force (IETF) system logging protocol specification.	1 for the initial version
timestamp	Time when the message was generated, in one of two representations: • *YYYY-MM-DDTHH:MM:SS.MSZ* is the year, month, day, hour, minute, second and millisecond in Universal Coordinated Time (UTC) • *YYYY-MM-DDTHH:MM:SS.MS+/-HH:MM* is the year, month, day, hour, minute, second and millisecond in local time; the hour and minute that follows the plus sign (+) or minus sign (-) is the offset of the local time zone from UTC	2007-02-15T09:17:15.719Z is 9:17 AM UTC on 15 February 2007. 2007-02-15T01:17:15.719 -08:00 is the same timestamp expressed as Pacific Standard Time in the United States.
hostname	Name of the host that originally generated the message.	router1
process	Name of the Junos OS process that generated the message.	mgd
processID	UNIX process ID (PID) of the Junos OS process that generated the message.	3046
TAG	Junos OS system log message tag, which uniquely identifies the message.	UI_DBASE_LOGOUT_EVENT
junos@2636.platform	An identifier for the type of hardware platform that generated the message. The junos@2636 prefix indicates that the platform runs Junos OS. It is followed by a dot-separated numerical identifier for the platform type. For a list of the identifiers, see Table 28 on page 75.	junos@2636.1.1.1.2.18 for the M120 router
variable-value-pairs	A variable-value pair for each element in the *message-text* string that varies depending on the circumstances that triggered the message. Each pair appears in the format ***variable = "value"***.	username="user"
message-text	English-language description of the event or error (omitted if the brief statement is included at the [**edit system syslog file *filename* structured-data**] hierarchy level). For the text for each message, see the chapters following System Log Messages.	User 'user' exiting configuration mode

By default, the structured-data version of a message includes English text at the end, as in the following example (which appears on multiple lines only for legibility):

```
<165>1 2007-02-15T09:17:15.719Z router1 mgd 3046 UI_DBASE_LOGOUT_EVENT
   [junos@2636.1.1.1.2.18 username="user"] User 'user' exiting configuration mode
```

When the brief statement is included at the [**edit system syslog file *filename* structured-data**] hierarchy level, the English text is omitted, as in this example:

```
<165>1 2007-02-15T09:17:15.719Z router1 mgd 3046 UI_DBASE_LOGOUT_EVENT
   [junos@2636.1.1.1.2.18 username="user"]
```

Table 27 on page 74 maps the codes that appear in the ***priority-code*** field to facility and severity level.

NOTE: Not all of the facilities and severities listed in Table 27 on page 74 can be included in statements at the [**edit system syslog**] hierarchy level (some are used by internal processes). For a list of the facilities and severity levels that can be included in the configuration, see “Specifying the Facility and Severity of Messages to Include in the Log” on page 15.

Table 27: Facility and Severity Codes in the priority-code Field

	Severity							
Facility (number)	emergency	alert	critical	error	warning	notice	info	debug
kernel (0)	1	1	2	3	4	5	6	7
user (1)	8	9	10	11	12	13	14	15
mail (2)	16	17	18	19	20	21	22	23
daemon (3)	24	25	26	27	28	29	30	31
authorization (4)	32	33	34	35	36	37	38	39
syslog (5)	40	41	42	43	44	45	46	47
printer (6)	48	49	50	51	52	53	54	55
news (7)	56	57	58	59	60	61	62	63
uucp (8)	64	65	66	67	68	69	70	71
clock (9)	72	73	74	75	76	77	78	79
authorization-private (10)	80	81	82	83	84	85	86	87
ftp (11)	88	89	90	91	92	93	94	95
ntp (12)	96	97	98	99	100	101	102	103

Table 27: Facility and Severity Codes in the priority-code Field *(continued)*

Facility (number)	Severity emergency	alert	critical	error	warning	notice	info	debug
security (13)	104	105	106	107	108	109	110	111
console (14)	112	113	114	115	116	117	118	119
local0 (16)	128	129	130	131	132	133	134	135
dfc (17)	136	137	138	139	140	141	142	143
local2 (18)	144	145	146	147	148	149	150	151
firewall (19)	152	153	154	155	156	157	158	159
pfe (20)	160	161	162	163	164	165	166	167
conflict-log (21)	168	169	170	171	172	173	174	175
change-log (22)	176	177	178	179	180	181	182	183
interactive-commands (23)	184	185	186	187	188	189	190	191

Table 28 on page 75 lists the numerical identifiers for routing platforms that appear in the ***platform*** field. The identifier is derived from the platform's SNMP object identifier (OID) as defined in the Juniper Networks routing platform MIB. For more information about OIDs, see the *Network Management Administration Guide*.

Table 28: Platform Identifiers in the platform Field

Identifier	Platform Name
1.1.1.2.1	M40 router
1.1.1.2.2	M20 router
1.1.1.2.3	M160 router
1.1.1.2.4	M10 router
1.1.1.2.5	M5 router
1.1.1.2.6	T640 routing node
1.1.1.2.7	T320 router
1.1.1.2.8	M40e router
1.1.1.2.9	M320 router

Table 28: Platform Identifiers in the platform Field *(continued)*

Identifier	Platform Name
1.1.1.2.10	M7i router
1.1.1.2.11	M10i router
1.1.1.2.13	J2300 Services Router
1.1.1.2.14	J4300 Services Router
1.1.1.2.15	J6300 Services Router
1.1.1.2.17	TX Matrix platform
1.1.1.2.18	M120 router
1.1.1.2.19	J4350 Services Router
1.1.1.2.20	J6350 Services Router
1.1.1.2.23	J2320 Services Router
1.1.1.2.24	J2350 Services Router
1.1.1.2.27	T1600 router
1.1.1.2.37	TX Matrix Plus platform
1.1.1.2.83	T4000 router

Examples: Displaying System Log Message Descriptions

Display the list of all currently available system log message descriptions:

```
  user@host> help syslog ?
```

```
Possible completions:
<syslog-tag>   Syslog tag
 . . .      . . .
BOOTPD_ARG_ERR   Command-line option was invalid
BOOTPD_BAD_ID   Request failed because assembly ID was unknown
BOOTPD_BOOTSTRING  tnp.bootpd provided boot string
BOOTPD_CONFIG_ERR  tnp.bootpd could not parse configuration file;
       used default settings
BOOTPD_CONF_OPEN  tnp.bootpd could not open configuration file
BOOTPD_DUP_REV   Extra boot string definitions for revision were
       ignored
---(more 4%)---
```

Display the list of all currently available system log message descriptions for tags that begin with the letters **ACCT** (there is no space between **ACCT** and the question mark, and some descriptions are shortened for legibility):

```
user@host> help syslog ACCT?
```

```
Possible completions:
<syslog-tag>       System log tag or regular expression
ACCT_ACCOUNTING_FERROR    Error occurred during file processing
ACCT_ACCOUNTING_FOPEN_ERROR   Open operation failed on file
ACCT_ACCOUNTING_SMALL_FILE_SIZE Maximum file size is smaller than ...
ACCT_BAD_RECORD_FORMAT    Record format does not match accounting profile
ACCT_CU_RTSLIB_ERROR    Error occurred obtaining current class usage ...
ACCT_FORK_ERR       Could not create child process
ACCT_FORK_LIMIT_EXCEEDED   Could not create child process because of limit
ACCT_GETHOSTNAME_ERROR    gethostname function failed
ACCT_MALLOC_FAILURE     Memory allocation failed
ACCT_UNDEFINED_COUNTER_NAME  Filter profile used undefined counter name
ACCT_XFER_FAILED      Attempt to transfer file failed
ACCT_XFER_POPEN_FAIL    File transfer failed
```

Display the description of the **UI_CMDLINE_READ_LINE** message:

```
user@host> help syslog UI_CMDLINE_READ_LINE
```

```
Name:    UI_CMDLINE_READ_LINE
Message:   User '<users>', command '<input>'
Help:    User entered command at CLI prompt
Description: The indicated user typed the indicated command at the CLI
     prompt and pressed the Enter key, sending the command string
     to the management process (mgd).
Type:    Event: This message reports an event, not an error
Severity:   info
```

CHAPTER 8

Configuring System Logging for a Security Device

Understanding System Logging for Security Devices

Junos OS supports configuring and monitoring of system log messages (also called *syslog messages*). You can configure files to log system messages and also assign attributes, such as severity levels, to messages. Reboot requests are recorded to the system log files, which you can view with the **show log** command.

This section contains the following topics:

Control Plane and Data Plane Logs

Junos OS generates separate log messages to record events that occur on the system's control and data planes.

- The control plane logs, also called system logs, include events that occur on the routing platform. The system sends control plane events to the **eventd** process on the Routing Engine, which then handles the events by using Junos OS policies, by generating system log messages, or both. You can choose to send control plane logs to a file, user terminal, routing platform console, or remote machine. To generate control plane logs, use the **syslog** statement at the **[system]** hierarchy level.

- The data plane logs, also called *security logs*, primarily include security events that are handled inside the data plane. Security logs can be in text or binary format, and they can be saved locally (event mode) or sent to an external server (stream mode). Binary format is required for stream mode and recommended to conserve log space in event mode.

  Note the following:

  - Security logs can be saved locally (on box) or externally (off box), but not both.
  - On SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices, the default and recommended mode that is supported for collecting/saving traffic logs is the stream mode (off-box). The system streams already-processed data plane events directly to external log servers, bypassing the Routing Engine. To specify binary format and an external server, see “Configuring Off-Box Binary Security Log Files” on page 95.
  - On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the default mode supported for collecting/saving traffic logs is the event mode (on-box). Data plane events are written to system log files in a similar manner to control plane events. To specify binary format for the security logs, see “Configuring On-Box Binary Security Log Files” on page 93.

Redundant System Log Server

Security system logging traffic intended for remote servers is sent through the network interface ports, which support two simultaneous system log destinations. Each system logging destination must be configured separately. When two system log destination addresses are configured, identical logs are sent to both destinations. While two destinations can be configured on any device that supports the feature, adding a second destination is primarily useful as a redundant backup for standalone and active/backup configured chassis cluster deployments.

The following redundant server information is available:

- Facility: **cron**
- Description: cron scheduling process
- Severity Level (from highest to lowest severity): **debug**
- Description: Software debugging messages

Related Documentation

- **log (Security) on page 120**
- Understanding Binary Format for Security Logs on page 81
- Setting the System to Send All Log Messages Through eventd on page 96
- Setting the System to Stream Security Logs Through Revenue Ports on page 97
- Sending System Log Messages to a File on page 96

- Understanding Stream Logging for Security Devices on page 81

Understanding Stream Logging for Security Devices

Junos OS supports forwarding logs using stream mode and event mode. All the categories can be configured for sending specific category logs to different log servers for stream mode log forwarding.

Stream mode log forwarding includes the following steps:

- An RTLOG system log message is generated by the data plane and is sent out from the Packet Forwarding Engine.
- An RTLOG system log message is generated by fpe process and is sent from Packet Forwarding Engine.
- An RTLOG system log message is generated by the Routing Engine unified threat management (utmd) process and is sent by rtlogd process from the Routing Engine.

On SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices, the default and recommended mode that is supported for collecting/saving traffic logs is the stream mode (off-box). The system streams already-processed data plane events directly to external log servers, bypassing the Routing Engine. To specify binary format and an external server, see "Configuring Off-Box Binary Security Log Files" on page 95.

For stream mode log forwarding, the transport protocol used between Packet Forwarding Engine and the log server can be UDP, TCP, or TLS. These transport protocols UDP, TCP, and TLS are configurable. The transport protocol used between the Routing Engine and the log server can only be UDP.

Related Documentation

- **log (Security) on page 120**
- Understanding Binary Format for Security Logs on page 81
- Setting the System to Send All Log Messages Through eventd on page 96
- Setting the System to Stream Security Logs Through Revenue Ports on page 97
- Sending System Log Messages to a File on page 96
- Monitoring System Log Messages with the J-Web Event Viewer on page 99

Understanding Binary Format for Security Logs

The Junos OS generates separate log messages to record events that occur on the system's control plane and data plane. The control plane monitors events that occur on the routing platform. Such events are recorded in system log messages. To generate system log messages, use the **syslog** statement at the **[system]** hierarchy level.

Data plane log messages, referred to as security log messages, record security events that the system handles directly inside the data plane. To generate security log messages, use the **log** statement at the **[security]** hierarchy level.

System log messages are maintained in log files in text-based formats, such as BSD Syslog, Structured Syslog, and WebTrends Enhanced Log Format (WELF).

Security log messages can also be maintained in text-based formats. Because security logging can produce large amounts of data, however, text-based log files can quickly consume storage and CPU resources. Depending on your implementation of security logging, a log file in a binary-based format can provide more efficient use of on-box or off-box storage and improved CPU utilization. Binary format for security log messages is available on all SRX Series devices.

When configured in event mode, security log messages generated in the data plane are directed to the control plane and stored locally on the device. Security log messages stored in binary format are maintained in a log file separate from that used to maintain system log messages. Events stored in a binary log file are not accessible with advanced log-scripting commands intended for text-based log files. A separate CLI operational command supports decoding, converting, and viewing binary log files that are stored locally on the device.

When configured in stream mode, security log messages generated in the data plane are streamed to a remote device. When these messages are stored in binary format, they are streamed directly to an external log collection server in a binary format. Externally-stored binary log files can only be read using Juniper Secure Analytics (JSA) or Security Threat Response Manager (STRM).

On SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices, the default and recommend mode that is supported for collecting/saving traffic logs is the stream mode (off-box). The system streams already-processed data plane events directly to external log servers, bypassing the Routing Engine. To specify binary format and an external server, see “Configuring Off-Box Binary Security Log Files” on page 95.

On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the default mode supported for collecting/saving traffic logs is the event mode (on-box). Data plane events are written to system log files in a similar manner to control plane events. To specify binary format for the security logs, see “Configuring On-Box Binary Security Log Files” on page 93.

For information about configuring on-box (event-mode) binary security logs, please see “Configuring On-Box Binary Security Log Files” on page 93. For information about configuring off-box (stream-mode) binary security logs, please see “Configuring Off-Box Binary Security Log Files” on page 95.

Related Documentation

- Understanding System Logging for Security Devices on page 79

Understanding On-Box Logging and Reporting

This topic describes the on-box logging and reporting CLI functionality and the design aspects of on-box reporting for the SRX devices.

Overview

On-box traffic logging to solid-state drives (SSDs) supports eight external log servers or files.

An all-in-one XML file is added that contains all the traffic logs information. The XML file also generates all the logging header files and traffic log related documents.

A new process (daemon) called *local log management daemon (llmd)* is supported in Services Processing Cards 0 (SPCs0) to handle on-box traffic logging. Traffic produced by flowd in SPCs is listed in traffics logs. The llmd saves these logs to the local SSD. Traffic logs are saved in the following four different formats:

- syslog
- sd-syslog
- welf
- binary

On-box reporting mechanism is an enhancement to the existing logging functionality. The existing logging functionality is modified to collect system traffic logs, analyzes the logs, and generate reports of these logs in the form of tables using the CLI. On-box reporting feature is intended to provide a simple and easy to use interface for viewing security logs. The on-box reports are easy to use J-Web pages of various security events in the form of tables and graphs. The reports allow the IT security management to identify security information at a glance, and quickly decide the actions to be taken.

NOTE: The on-box reporting feature is enabled by default when you load the factory-default configurations on the SRX Series device with Junos OS Release 15.1X49-D100 or later.

If you are upgrading your SRX Series device from a Junos OS Release prior to Junos OS 15.1X49-D100, then the SRX device inherits the existing configuration and the on-box reporting feature is disabled by default. You need to run the **set security log report** command and the **set security log mode stream** command to enable the on-box reporting feature on the device that are upgraded.

After the log message is recorded, the log is stored within a log file which is then stored in the database table of the RE for further analysis (on SRX300, SRX320, SRX340, SRX345, and SRX550M devices) or on the SSD card for further analysis (on SRX1500, SRX4100, and SRX4200 devices).

NOTE: This feature supports receiving top most reports based on count or volume of the session or the type of log, captures events occurring in each second within a specified time range, captures log content for a specified CLI condition. Various CLI conditions like “summary”, top”, “in-detail”, and “in-interval” are used to generate reports. You can generate only one report at one time using the CLI. All the CLI conditions cannot be used at the same time. You can generate only one report at one time using the CLI.

The benefits of this feature are:

- Reports are stored locally on the SRX Series device and there is no requirement for separate devices or tools for logs and reports storage.
- The on-box reports are easy-to-use J-Web pages of various security events in the form of tables and graphs.
- Provides a simple and easy-to-use interface for viewing security logs.
- The reports generated enables the IT security management team to identify security information at a glance and quickly decide the actions to be taken.

The on-box reporting feature supports:

- Generating reports based on the requirements. For example: count or volume of the session, types of logs for activities such as IDP, UTM, IPsec VPN.
- Capturing real-time events within a specified time range.
- Capturing all the network activities in a logical, organized, and easy-to-understand format based on various CLI specified conditions.

Understanding On-box logging and Reporting

In the on-box reporting mechanism, CLI is used to fetch the reporting data from the device. The SRX series device collects and saves all the required logs. These recorded logs are then used for further analysis to calculate and generate reports in the form of tables using the CLI. The data generated using CLI in the form of reports can be further retrieved in the form of tables and graphs in J-Web. The reports generated are easy-to-understand tables and graphs in J-Web. Thorough analysis of logs is performed (based on session types) for features such as screen, IDP, UTM and IPSec.

You can define filters for the log data that is reported on based on the following criteria:

NOTE: **The top, in-detail, and in-interval conditions cannot be used at the same time.**

- **top** *<number>*—This option allow you to generate reports for top security events as specified in the command. for example: top 5 IPS attacks or top 6 URLs detected through UTM.
- **in-detail** *<number>*—This option allow you to generate detail log content.
- **in-interval** *<time-period>*—This option allows you to generate the events logged between certain time intervals.
- **summary**—This option allows you to generate the summary of the events. In this way, you can fine-tune the report to your needs, and displays only the data that you want to use.

The maximum in-interval number which shows the count in intervals is 30. If large duration is specified, then the counters are assembled to ensure the maximum in-interval is less than 30.

Both in-detail and summary have the “all” option, since different table have different attribute (like session table does not have the attribute “reason” but UTM has), the “all” option does not have any filter except start-time and stop-time. If there is any other filter other than start time and stop time then an error is displayed.

For example: root@kujang> show security log report in-detail all reason reason1

```
error: "query condition error"
```

The application firewall logs for application and user visibility will list applications and nested applications. When the logs of these features list nested applications then nested applications are listed in J-Web. When the logs list nested applications as not-applicable or unknown then only the applications are listed in J-Web.

Use the following CLI commands for application and user visibility for all the applications and nested applications listing:

- For top nested-application by count—**show security log report top session-close top-number <number> group-by application order-by count with user**
- For top nested-application by volume—**show security log report top session-close top-number <number> group-by application order-by volume with user**
- For top user by count with nested application—**show security log report top session-close top-number <number> group-by user order-by count with application**

On-Box Reporting Features

The on-box reporting feature supports:

- **Sqlite3 support as a library**—sqlite3 was not supported prior to Junos OS release 15.1X49-D100. Starting with Junos OS Release 15.1X49-D100, an SQL log database (SQLite Version 3) is used by the daemons running on the RE as well as other potential modules to store logs on SRX Series devices.
- **Running llmd in both Junos OS and Linux OS**—The forwarding daemon (flowd) decodes database index from binary logs and sends both index and log to the local log management daemon (llmd).

  On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, llmd runs in Junos OS. On SRX1500, SRX4100, and SRX4200 devices, llmd runs in Linux. So, for supporting llmd to run in both Junos OS and Linux OS, the llmd code directory is moved from the Linux side to the Junos OS side.
- **Storing of logs into specified table of the sqlite3 database by llmd**— A new syslog daemon is introduced to collect local logs on SRX Series devices and saving them into the database.
  - **Database table definition**—For session logs, the data types are source-address, destination-address, application, user, and so on. For logs related to security features, the data types are attack-name, URL, profile protocol, and so on. Therefore, different tables are designed to store different types of logs to help improve the performance and save disk space. SRX device creates a database table for each log type, when log data is recorded.
  - **Database table rotation**—Each type of database table has its maximum record number that is device specific. When the table record number reaches the limitation, new logs replace the oldest logs.
- **Calculating and displaying the reports that are triggered by CLI**—The reports from the database are received from the CLI as the interface. Using the CLI, you can calculate and display the reporting details.

Chassis Cluster Scenario

For on-box reporting in a chassis cluster, the logs are stored in the local disk on which the device is processing active traffic. These logs are not synchronized to the chassis cluster peer.

Each node is responsible to store logs when each node is processing active traffic. In case of active/passive mode, only the active node processes the traffic and logs are also stored only in the active node. In case of failover, the new active node is processes the traffic and stores logs in its local disk. In case of active/active mode, each node processes its own traffic and logs are stored in the respective nodes.

Related Documentation

- report on page 133

Monitoring Reports

On-box reporting offers a comprehensive reporting facility where your security management team can spot a security event when it occurs, immediately access and review pertinent details about the event, and quickly decide appropriate remedial action. The J-Web reporting feature provides one- or two-page reports that are equivalent to a compilation of numerous log entries.

This section contains the following topics:

- Threats Monitoring Report on page 87
- Traffic Monitoring Report on page 91

Threats Monitoring Report

Purpose Use the Threats Report to monitor general statistics and activity reports of current threats to the network. You can analyze logging data for threat type, source and destination details, and threat frequency information. The report calculates, displays, and refreshes the statistics, providing graphic presentations of the current state of the network.

Action To view the Threats Report:

1. Click **Threats Report** in the bottom right of the Dashboard, or select **Monitor>Reports>Threats** in the J-Web user interface. The Threats Report appears.

2. Select one of the following tabs:
   - **Statistics** tab. See Table 29 on page 87 for a description of the page content.
   - **Activities** tab. See Table 30 on page 89 for a description of the page content.

Table 29: Statistics Tab Output in the Threats Report

Field	Description
General Statistics Pane	
Threat Category	One of the following categories of threats: • Traffic • IDP • Content Security ◦ Antivirus ◦ Antispam ◦ Web Filter—Click the Web filter category to display counters for 39 subcategories. ◦ Content Filter • Firewall Event

Table 29: Statistics Tab Output in the Threats Report *(continued)*

Field	Description
Severity	Severity level of the threat: • emerg • alert • crit • err • warning • notice • info • debug
Hits in past 24 hours	Number of threats encountered per category in the past 24 hours.
Hits in current hour	Number of threats encountered per category in the last hour.
Threat Counts in the Past 24 Hours	
By Severity	Graph representing the number of threats received each hour for the past 24 hours sorted by severity level.
By Category	Graph representing the number of threats received each hour for the past 24 hours sorted by category.
X Axis	Twenty-four hour span with the current hour occupying the right-most column of the display. The graph shifts to the left every hour.
Y Axis	Number of threats encountered. The axis automatically scales based on the number of threats encountered.
Most Recent Threats	
Threat Name	Names of the most recent threats. Depending on the threat category, you can click the threat name to go to a scan engine site for a threat description.
Category	Category of each threat: • Traffic • IDP • Content Security ◦ Antivirus ◦ Antispam ◦ Web Filter ◦ Content Filter • Firewall Event
Source IP/Port	Source IP address (and port number, if applicable) of the threat.
Destination IP/Port	Destination IP address (and port number, if applicable) of the threat.

Table 29: Statistics Tab Output in the Threats Report *(continued)*

Field	Description
Protocol	Protocol name of the threat.
Description	Threat identification based on the category type: • Antivirus—URL • Web filter—category • Content filter—reason • Antispam—sender e-mail
Action	Action taken in response to the threat.
Hit Time	Time the threat occurred.
Threat Trend in past 24 hours	
Category	Pie chart graphic representing comparative threat counts by category: • Traffic • IDP • Content Security ◦ Antivirus ◦ Antispam ◦ Web Filter ◦ Content Filter • Firewall Event
Web Filter Counters Summary	
Category	Web filter count broken down by up to 39 subcategories. Clicking on the Web filter listing in the General Statistics pane opens the Web Filter Counters Summary pane.
Hits in past 24 hours	Number of threats per subcategory in the last 24 hours.
Hits in current hour	Number of threats per subcategory in the last hour.

Table 30: Activities Tab Output in the Threats Report

Field	Function
Most Recent Virus Hits	
Threat Name	Name of the virus threat. Viruses can be based on services, like Web, FTP, or e-mail, or based on severity level.

Table 30: Activities Tab Output in the Threats Report *(continued)*

Field	Function
Severity	Severity level of each threat: • emerg • alert • crit • err • warning • notice • info • debug
Source IP/Port	IP address (and port number, if applicable) of the source of the threat.
Destination IP/Port	IP address (and port number, if applicable) of the destination of the threat.
Protocol	Protocol name of the threat.
Description	Threat identification based on the category type: • Antivirus—URL • Web filter—category • Content filter—reason • Antispam—sender e-mail
Action	Action taken in response to the threat.
Last Hit Time	Last time the threat occurred.
Most Recent Spam E-Mail Senders	
From e-mail	E-mail address that was the source of the spam.
Severity	Severity level of the threat: • emerg • alert • crit • err • warning • notice • info • debug
Source IP	IP address of the source of the threat.
Action	Action taken in response to the threat.
Last Send Time	Last time that the spam e-mail was sent.

Table 30: Activities Tab Output in the Threats Report *(continued)*

Field	Function
Recently Blocked URL Requests	
URL	URL request that was blocked.
Source IP/Port	IP address (and port number, if applicable) of the source.
Destination IP/Port	IP address (and port number, if applicable) of the destination.
Hits in current hour	Number of threats encountered in the last hour.
Most Recent IDP Attacks	
Attack	
Severity	Severity of each threat: • emerg • alert • crit • err • warning • notice • info • debug
Source IP/Port	IP address (and port number, if applicable) of the source.
Destination IP/Port	IP address (and port number, if applicable) of the destination.
Protocol	Protocol name of the threat.
Action	Action taken in response to the threat.
Last Send Time	Last time the IDP threat was sent.

Traffic Monitoring Report

Purpose Monitor network traffic by reviewing reports of flow sessions over the past 24 hours. You can analyze logging data for connection statistics and session usage by a transport protocol.

Action To view network traffic in the past 24 hours, select **Monitor>Reports>Traffic** in the J-Web user interface. See Table 31 on page 92 for a description of the report.

Table 31: Traffic Report Output

Field	Description
Sessions in Past 24 Hours per Protocol	
Protocol Name	Name of the protocol. To see hourly activity by protocol, click the protocol name and review the “Protocol activities chart” in the lower pane. • TCP • UDP • ICMP
Total Session	Total number of sessions for the protocol in the past 24 hours.
Bytes In (KB)	Total number of incoming bytes in KB.
Bytes Out (KB)	Total number of outgoing bytes in KB.
Packets In	Total number of incoming packets.
Packets Out	Total number of outgoing packets.
Most Recently Closed Sessions	
Source IP/Port	Source IP address (and port number, if applicable) of the closed session.
Destination IP/Port	Destination IP address (and port number, if applicable) of the closed session.
Protocol	Protocol of the closed session. • TCP • UDP • ICMP
Bytes In (KB)	Total number of incoming bytes in KB.
Bytes Out (KB)	Total number of outgoing bytes in KB.
Packets In	Total number of incoming packets.
Packets Out	Total number of outgoing packets.
Timestamp	The time the session was closed.
Protocol Activities Chart	
Bytes In/Out	Graphic representation of traffic as incoming and outgoing bytes per hour. The byte count is for the protocol selected in the Sessions in Past 24 Hours per Protocol pane. Changing the selection causes this chart to refresh immediately.
Packets In/Out	Graphic representation of traffic as incoming and outgoing packets per hour. The packet count is for the protocol selected in the Sessions in Past 24 Hours per Protocol pane. Changing the selection causes this chart to refresh immediately.

Table 31: Traffic Report Output *(continued)*

Field	Description
Sessions	Graphic representation of traffic as the number of sessions per hour. The session count is for the protocol selected in the Sessions in Past 24 Hours per Protocol pane. Changing the selection causes this chart to refresh immediately.
X Axis	One hour per column for 24 hours.
Y Axis	Byte, packet, or session count.
Protocol Session Chart	
Sessions by Protocol	Graphic representation of the traffic as the current session count per protocol. The protocols displayed are TCP, UDP, and ICMP.

Related Documentation

- *Monitoring Overview*
- *Monitoring Interfaces*

Configuring On-Box Binary Security Log Files

SRX Series devices have two types of log: system logs and security logs. System logs record control plane events, for example admin login to the device. For more about system logs, please see "Junos OS System Log Overview" on page 3. Security logs, also known as traffic logs, record data plane events regarding specific traffic handling, for example when a security policy denies certain traffic due to some violation of the policy. For more information about security logs, please see "Understanding System Logging for Security Devices" on page 79.

On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the default mode supported for collecting/saving traffic logs is the event mode (on-box). Data plane events are written to system log files in a similar manner to control plane events.

The two types of log can be collected and saved either on-box or off-box. The procedure below explains how to configure security logs in binary format for on-box (event-mode) logging.

You can configure security files in binary format using the **log** statement at the **[security]** hierarchy level.

The following procedure specifies binary format for event-mode security logging, and defines the log filename, path, and log file characteristics. For stream-mode, off-box security logging, please see "Configuring Off-Box Binary Security Log Files" on page 95.

1. Specify the logging mode and the format for the log file. For on-box, event-mode logging:

   ```
   set security log mode event
   set security log format binary
   ```

NOTE: If system logging has been set to send system logs to an external destination, security logs will also be sent to that destination when using security log event-mode. More information about sending system logs to an external destination is available here "Examples: Configuring System Logging" on page 29.

NOTE: Off-box and on-box security logging modes cannot be enabled simultaneously.

2. Optionally, define a log filename and a path. By default, the file bin_messages is created in the /var/log directory.

   ```
   set security log file name security-binary-log
   set security log file path security/log-folder
   ```

3. Optionally, change the maximum size of the log file and the maximum number of log files that can be archived. By default the maximum size of the log file is 3 MB, and a total of three log files can be archived.

   ```
   set security log file size 5
   set security log file files 5
   ```

4. Optionally, select the hpl flag to enable diagnostic traces for binary logging. The prefix smf_hpl identifies all binary logging traces.

   ```
   set security log traceoptions flag hpl
   ```

5. View the content of the event-mode log file stored on the device.

   ```
   show security log file
   ```

   NOTE: The **show security log** command displays event-mode security log messages if they are in a text-based format. The **show security log file** command displays event-mode security log messages if they are in binary format.

   Use the following command to clear the content of the binary event-mode security log file.

   ```
   clear security log file
   ```

Related Documentation

- Understanding Binary Format for Security Logs on page 81
- Setting the System to Send All Log Messages Through eventd on page 96

Configuring Off-Box Binary Security Log Files

SRX Series devices have two types of log: system logs and security logs. System logs record control plane events, for example admin login to the device. For more about system logs, please see "Junos OS System Log Overview" on page 3. Security logs, also known as traffic logs, record data plane events regarding specific traffic handling, for example when a security policy denies certain traffic due to some violation of the policy. For more information about security logs, please see "Understanding System Logging for Security Devices" on page 79.

On SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices, the default and recommend mode that is supported for collecting/saving traffic logs is the stream mode (off-box). The system streams already-processed data plane events directly to external log servers, bypassing the Routing Engine. To specify binary format and an external server, see "Configuring Off-Box Binary Security Log Files" on page 95.

The two types of log can be collected and saved either on-box or off-box. The procedure below explains how to configure security logs in binary format for off-box (stream-mode) logging.

You can configure security files in binary format using the **log** statement at the **[security]** hierarchy level.

The following procedure specifies binary format for stream-mode security logging, and defines the log filename, path, and log file characteristics. For event-mode, on-box security logging, please see "Configuring On-Box Binary Security Log Files" on page 93.

1. Specify the logging mode and the format for the log file. For off-box, stream-mode logging:

   ```
   set security log mode stream
   set security log stream test-stream format binary host 1.3.54.22
   ```

   NOTE: Off-box and on-box security logging modes cannot be enabled simultaneously.

2. For off-box security logging, specify the source address, which identifies the SRX Series device that generated the log messages. The source address is required.

   ```
   set security log source-address 2.3.45.66
   ```

3. Optionally, define a log filename and a path. By default, the file bin_messages is created in the /var/log directory.

   ```
   set security log file name security-binary-log
   set security log file path security/log-folder
   ```

4. Optionally, change the maximum size of the log file and the maximum number of log files that can be archived. By default the maximum size of the log file is 3 MB, and a total of three log files can be archived.

   ```
   set security log file size 5
   set security log file files 5
   ```

5. Optionally, select the hpl flag to enable diagnostic traces for binary logging. The prefix smf_hpl identifies all binary logging traces.

   ```
   set security log traceoptions flag hpl
   ```

6. View the content of the event-mode log file stored on the device using either Juniper Secure Analytics (JSA) or Security Threat Response Manager (STRM).

Related Documentation

- Understanding Binary Format for Security Logs on page 81
- Setting the System to Send All Log Messages Through eventd on page 96
- Setting the System to Stream Security Logs Through Revenue Ports on page 97

Sending System Log Messages to a File

You can direct system log messages to a file on the CompactFlash (CF) card. The default directory for log files is **/var/log**. To specify a different directory on the CF card, include the complete pathname.

Create a file named **security**, and send log messages of the **authorization** class at the severity level **info** to the file.

To set the filename, the facility, and severity level:

```
{primary:node0}
user@host# set system syslog file security authorization info
```

Related Documentation

- Understanding System Logging for Security Devices on page 79
- Understanding Binary Format for Security Logs on page 81
- Setting the System to Send All Log Messages Through eventd on page 96
- Setting the System to Stream Security Logs Through Revenue Ports on page 97
- Monitoring System Log Messages with the J-Web Event Viewer on page 99

Setting the System to Send All Log Messages Through eventd

The **eventd** process of logging configuration is most commonly used for Junos OS. In this configuration, control plane logs and data plane, or security, logs are forwarded from the data plane to the Routing Engine control plane **rtlogd** process. The **rtlogd** process then either forwards syslog or sd-syslog-formatted logs to the **eventd** process or the WELF-formatted logs to the external or remote WELF log collector.

To send all log messages through **eventd**:

1. Set the **eventd** process to handle security logs and send them to a remote server.

   ```
   {primary:node0}
   user@host# set security log mode event
   ```

2. Configure the server that will receive the system log messages.

   ```
   {primary:node0}
   user@host# set system syslog host hostname any any
   ```

   where ***hostname*** is the fully qualified hostname or IP address of the server that will receive the logs.

NOTE: To send duplicate logs to a second remote server, repeat the command with a new fully qualified *hostname* or IP address of a second server.

If your deployment is an active/active chassis cluster, you can also configure security logging on the active node to be sent to separate remote servers to achieve logging redundancy.

To rename or redirect one of the logging configurations, you need to delete and recreate it. To delete a configuration:

```
{primary:node0}
user@host# delete security log mode event
```

Related Documentation

- Understanding System Logging for Security Devices on page 79
- Understanding Binary Format for Security Logs on page 81
- Setting the System to Stream Security Logs Through Revenue Ports on page 97
- Sending System Log Messages to a File on page 96
- Monitoring System Log Messages with the J-Web Event Viewer on page 99

Setting the System to Stream Security Logs Through Revenue Ports

You can increase the number of data plane, or security, logs that are sent by modifying the manner in which they are sent. When the logging mode is set to **stream**, security logs generated in the data plane are streamed out a revenue traffic port directly to a remote server.

To use the **stream** mode, enter the following commands:

```
{primary:node0}
user@host# set security log source-address source-address
```

```
user@host# set security log stream streamname format (syslog|sd-syslog|welf) category
   (all|content-security) host ipaddr
```

where *source-address* is the IP address of the source machine; **syslog**, **sd-syslog** (structured system logging messages) and **welf** are logging formats; **all** and **content-security** are the categories of logging; and *ipaddr* is the IP address of the server to which the logs will be streamed.

NOTE: WELF logs must be streamed through a revenue port because the eventd process does not recognize the WELF format. The category must be set to content-security. For example:

```
{primary:node0}
user@host# set security log stream securitylog1 format
   welf category content-security host 10.121.23.5
```

To send duplicate logs to a second remote server, repeat the command with a new *ipaddr*. If your deployment is an active/active chassis cluster, you can also configure security logging on the active node to be sent to separate remote servers to achieve logging redundancy.

Starting in Junos OS Release 15.1X49-D70, on SRX1500, SRX4100, and SRX4200 Series devices and vSRX instances, the **set security log stream ${*stream_name*}** command is required to configure the stream log. The source address and source interface attributes are no longer required. On SRX300, SRX320, SRX340, and SRX345 Series devices, the **set security log stream ${*stream_name*} host ${host_IP}** command is required to configure the stream log file with the source address and source interface attributes configuration.

Release History Table

Release	Description
15.1X49-D70	Starting in Junos OS Release 15.1X49-D70, on SRX1500, SRX4100, and SRX4200 Series devices and vSRX instances, the **set security log stream ${*stream_name*}** command is required to configure the stream log. The source address and source interface attributes are no longer required. On SRX300, SRX320, SRX340, and SRX345 Series devices, the **set security log stream ${*stream_name*} host ${host_IP}** command is required to configure the stream log file with the source address and source interface attributes configuration.

Related Documentation

- Understanding System Logging for Security Devices on page 79
- Understanding Binary Format for Security Logs on page 81
- Setting the System to Send All Log Messages Through eventd on page 96
- Sending System Log Messages to a File on page 96
- Monitoring System Log Messages with the J-Web Event Viewer on page 99

Monitoring System Log Messages with the J-Web Event Viewer

Purpose Monitor errors and events that occur on the device.

Action Select **Monitor>Events and Alarms>View Events** in the J-Web user interface.

The J-Web View Events page displays the following information about each event:

- Process—System process that generated the error or event.
- Severity— A severity level indicates how seriously the triggering event affects routing platform functions. Only messages from the facility that are rated at that level or higher are logged. Possible severities and their corresponding color code are:
  - Debug/Info/Notice (Green)—Indicates conditions that are not errors but are of interest or might warrant special handling.
  - Warning (Yellow)—Indicates conditions that warrant monitoring.
  - Error (Blue)—Indicates standard error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.
  - Critical (Pink)—Indicates critical conditions, such as hard drive errors.
  - Alert (Orange)—Indicates conditions that require immediate correction, such as a corrupted system database.
  - Emergency (Red)—Indicates system panic or other conditions that cause the routing platform to stop functioning.
- Event ID—Unique ID of the error or event. The prefix on each code identifies the generating software process. The rest of the code indicates the specific event or error.
- Event Description—Displays a more detailed explanation of the message.
- Time—Time that the error or event occurred.

To control which errors and events are displayed in the list, use the following options:

- System Log File—Specify the name of the system log file that records the errors and events.
- Process—Specify the system processes that generate the events you want to display. To view all the processes running on your system, enter the **show system processes** CLI command.
- Date From—Specify the beginning of the date range that you want to monitor. Set the date using the calendar pick tool.
- To—Specify the end of the date range that you want to monitor. Set the date using the calendar pick tool.
- Event ID—Specify the specific ID of the error or event that you want to monitor.
- Description—Enter a description for the errors or events.
- Search—Fetches the errors and events specified in the search criteria.

- Reset—Clears the cache of errors and events that were previously selected.
- Generate Report—Creates an HTML report based on the specified parameters.

Related Documentation

- Understanding System Logging for Security Devices on page 79
- Understanding Binary Format for Security Logs on page 81
- *Monitoring Overview*
- *Monitoring Interfaces*

CHAPTER 9

Configuration Statements and Operational Commands

Configuration Statements

allow-duplicates

Syntax

```
allow-duplicates;
```

Hierarchy Level

[edit logical-systems *logical-system-name* system syslog],
[edit logical-systems *logical-system-name* system syslog file *file-name*],
[edit logical-systems *logical-system-name* system syslog host *host-name*],
[edit logical-systems *logical-system-name* system syslog user *user-name*],
[edit system syslog],
[edit system syslog file *file-name*],
[edit system syslog host *host-name*],
[edit system syslog user *user-name*],

Release Information

Statement introduced in Junos OS Release 11.1.
Logical systems support introduced in Junos OS Release 11.4.

Description

Specify whether to allow the repeated messages in the system log output files. This can be set either at global configuration level or for individual file, host, or user. By default, this parameter is set to disable.

Options

file—Name of the file to log messages

host —Host to receive the messages

user—User to receive the notification of the event

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- syslog (System) on page 139

archive (All System Log Files)

Syntax

```
archive <files number> <size size> <start-timetime> <transfer-interval interval>
  <binary-data | no-binary-data>;
  <world-readable | no-world-readable> ;
```

Hierarchy Level [edit system syslog]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure archiving properties for all system log files.

Options

files ***number***—Maximum number of archived log files to retain. When the Junos OS logging utility has written a defined maximum amount of data to a log file ***logfile***, it closes the file, compresses it, and renames it ***logfile*.0.gz** (the amount of data is determined by the **size** statement at this hierarchy level). The utility then opens and writes to a new file called ***logfile***. When the new file reaches the maximum size, the ***logfile*.0.gz** file is renamed to ***logfile*.1.gz**, and the new file is closed, compressed, and renamed ***logfile*.0.gz**. By default, the logging facility creates up to ten archive files in this manner. Once the maximum number of archive files exists, each time the active log file reaches the maximum size, the contents of the oldest archive file are lost (overwritten by the next oldest file).

Range: 1 through 1000

Default: 10 files

size ***size***—Maximum amount of data that the Junos OS logging utility writes to a log file ***logfile*** before archiving it (closing it, compressing it, and changing its name to ***logfile*.0.gz**). The utility then opens and writes to a new file called ***logfile***.

Syntax: ***x*** **k** to specify the number of kilobytes, ***x*** **m** for the number of megabytes, or ***x*** **g** for the number of gigabytes

Range: 64 KB through 1 GB

Default:

- 128 KB for EX Series switches
- 1 MB for M Series, MX Series, and T Series routers, OCX Series, and the QFX3500 switch
- 10 MB for TX Matrix and TX Matrix Plus routers

binary-data | no-binary-data—Mark file as containing binary data. This allows proper archiving of binary files, such as WTMP files (login records for UNIX based systems)..

Default: **no-binary-data**

world-readable | no-world-readable—Grant all users permission to read archived log files, or restrict the permission only to the **root** user and users who have the Junos OS **maintenance** permission.

Default: no-world-readable

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Specifying Log File Size, Number, and Archiving Properties on page 19

archive (Individual System Log File)

Syntax archive <archive-sites (*ftp-url* <password *password*>)> <files *number*> <size *size*> <start-time "*YYYY-MM-DD.hh:mm*"> <transfer-interval *minutes*> <world-readable | no-world-readable>;

Hierarchy Level [edit system syslog file *filename*]

Release Information Statement introduced before Junos OS Release 7.4.
start-time and **transfer-interval** statements introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure archiving properties for a specific system log file.

Options **archive-sites** ***site-name***—FTP URL representing the destination for the archived log file (for information about how to specify valid FTP URLs, see *Format for Specifying Filenames and URLs in Junos OS CLI Commands*). If more than one site name is configured, a list of archive sites for the system log files is created. When a file is archived, the router attempts to transfer the file to the first URL in the list, moving to the next site only if the transfer does not succeed. The log file is stored at the archive site with the filename specified at the **[edit system syslog]** hierarchy level.

files ***number***—Maximum number of archived log files to retain. When the Junos OS logging utility has written a defined maximum amount of data to a log file ***logfile***, it closes the file, compresses it, and renames it ***logfile*.0.gz** (the amount of data is determined by the **size** statement at this hierarchy level). The utility then opens and writes to a new file called ***logfile***. When the new file reaches the maximum size, the ***logfile*.0.gz** file is renamed to ***logfile*.1.gz**, and the new file is closed, compressed, and renamed ***logfile*.0.gz**. By default, the logging facility creates up to ten archive files in this manner. Once the maximum number of archive files exists, each time the active log file reaches the maximum size, the contents of the oldest archive file are lost (overwritten by the next oldest file).

Range: 1 through 1000

Default: 10 files

password ***password***—Password for authenticating with the site specified by the **archive-sites** statement.

size ***size***—Maximum amount of data that the Junos OS logging utility writes to a log file ***logfile*** before archiving it (closing it, compressing it, and changing its name to ***logfile*.0.gz**). The utility then opens and writes to a new file called ***logfile***.

Syntax: ***x*k** to specify the number of kilobytes, ***x*m** for the number of megabytes, or ***x*g** for the number of gigabytes

Range: 64 KB through 1 GB

Default: 128 KB for J Series routers; 1 MB for M Series, MX Series, and T Series routers, and the QFX3500 switch; 10 MB for TX Matrix and TX Matrix Plus routers

start-time "*YYYY-MM-DD.hh:mm*"—Date and time in the local time zone for a one-time transfer of the active log file to the first reachable site in the list of sites specified by the **archive-sites** statement.

transfer-interval *interval*—Interval at which to transfer the log file to an archive site.

Range: 5 through **2880** minutes

world-readable | no-world-readable—Grant all users permission to read archived log files, or restrict the permission only to the **root** user and users who have the Junos OS **maintenance** permission.

Default: no-world-readable

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Specifying Log File Size, Number, and Archiving Properties on page 19

cache (Security Log)

Syntax

```
cache {
  exclude exlude-name {
    destination-address destination-address;
    destination-port destination-port;
    event-id event-id;
    failure;
    interface-name interface-name;
    policy-name policy-name;
    process process-name;
    protocol protocol;
    source-address source-address;
    source-port source-address;
    success;
    user-name user-name;
  }
  limit value;
}
```

Hierarchy Level [edit security log]

Release Information Statement modified in Junos OS Release 9.2.

Description Cache security log events in the audit log buffer.

Options The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- syslog (System) on page 139

category (Security Logging)

Syntax

category (all | content-security | fw-auth | screen | alg | nat | flow | sctp | gtp | ipsec | idp |
rtlog | pst-ds-lite | appqos | secintel)

Hierarchy Level

[edit security log stream *stream-name*]

Release Information

Statement introduced in Junos OS Release 10.0. Statement modified in Junos OS Release 15.1X49-D40.

Description

Set the category of logging to **all** or **content-security**. Note that for the WELF format, the category must be set to **content-security**.

Options

- **all**—All events are logged. By default, all the events listed in the **category** parameter are logged.
- **content-security**—Only content security events are logged.
- **fw-auth**—Firewall authentication events are logged.
- **screen**—Screen events are logged.
- **alg**—Application Layer Gateway (ALG) events are logged.
- **nat**—Network Address Translation (NAT) events are logged.
- **flow**—Flow events are logged.
- **sctp**—Stream Control Transmission Protocol (SCTP) events are logged.
- **gtp**—GPRS Tunneling Protocol (GTP) events are logged.
- **ipsec**—IPsec events are logged.
- **idp**—Intrusion Detection and Prevention (IDP) events are logged.
- **rtlog**—RTLOG system log events are logged.
- **pst-ds-lite**—PST dual-stack lite (DS-Lite) events are logged.
- **appqos**—Application quality of service (AppQoS) events are logged.
- **secintel**—Juniper Networks Security Intelligence (SecIntel) events are logged.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- *AppSecure Services Feature Guide for Security Devices*
- *Logical Systems Feature Guide for Security Devices*

console (System Logging)

Syntax

```
console {
  facility severity;
}
```

Hierarchy Level

[edit system syslog]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the logging of system messages to the system console. Log messages include priority information, which is information about log messages' facility and severity levels.

Options

facility—Class (type) of messages to log. To specify multiple classes, include multiple ***facility severity*** statements.

severity—Severity of the messages that belong to the facility specified by the paired ***facility*** name. Messages with severities of the specified level and higher are logged. You can specify the minimum severity level of a message.

NOTE: For a list of the facilities and message severities, see Table 3 on page 5.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Directing System Log Messages to the Console on page 19
- System Log Explorer

destination-override

Syntax

```
destination-override {
  syslog host ip-address;
}
```

Hierarchy Level

[edit system tracing]

Release Information

Statement introduced in Junos OS Release 9.2.

Description

This option overrides the system-wide configuration under **[edit system tracing]** and has no effect if system tracing is not configured.

Options

These options specify the system logs and the host to which remote tracing output is sent:

- **syslog**—Specify the system process log files to send to the remote tracing host.
- **host** ***ip-address***—Specify the IP address to which to send tracing information.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Tracing and Logging Operations*
- tracing on page 145

event-rate

Syntax event-rate *rate;*

Hierarchy Level [edit security log]

Release Information Statement introduced in Junos OS Release 10.0.

Description Limits the rate at which logs will be streamed per second.

On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the default mode supported for collecting/saving traffic logs is the event mode (on-box). Data plane events are written to system log files in a similar manner to control plane events. To specify binary format for the security logs, see "Configuring On-Box Binary Security Log Files" on page 93.

NOTE: For devices with multicore systems that use SPUs, each SPU is programmed with the configured-rate, which results in an aggregate-rate proportional to the number of SPUs.

Resulting aggregate-rate = configured-rate * number-of-SPUs

For example, to configure an aggregate-rate of 1000 packets/second to the device with multicore system with 10 SPUs, then each SPU is to be programmed with configured-rate of 100 packets/second.

Options *rate*—Rate at which logs will be streamed per second.

Range: 0 through 1500 logs per second

Default: 1500 logs per second

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- syslog (System) on page 139

exclude (Security Log)

Syntax

```
exclude exlude-name {
  destination-address destination-address;
  destination-port destination-port;
  event-id event-id;
  failure;
  interface-name interface-name;
  policy-name policy-name;
  process process-name;
  protocol protocol;
  source-address source-address;
  source-port source-port;
  success;
  user-name user-name;
}
```

Hierarchy Level [edit security log cache]

Release Information Statement introduced in Junos OS Release 11.2.

Description Configure a list of auditable events that can be excluded from the audit log.

Options

- **destination-ip *destination-address***—Destination IP address.
- **destination-port *destination-port***—Destination port number.
- **event-id *event-id***—Error message identification number.
- **failure**—Failed audit event logs.
- **interface-name *interface-name***—Name of the interface.
- **policy-name *policy-name***—Policy name filter.
- **process *process-name***—Process that generated the event.
- **protocol *protocol***—Protocol that generated the event.
- **source-ip *source-address***—Source IP address.
- **source-port *source-port***—Source port number.
- **success**—Successful audit event logs.
- **username *user-name***—User name filter.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- show security log on page 162
- clear security log on page 149

exclude-hostname

Syntax exclude-hostname;

Hierarchy Level [edit system syslog host *hostname*]

Release Information Statement introduced in Junos OS Release 13.2

Description Disable logging of hostname in the message directed to remote host.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Directing System Log Messages to a Remote Machine or the Other Routing Engine on page 31

explicit-priority

Syntax explicit-priority;

Hierarchy Level [edit logical-systems *logical-system-name* system syslog file *filename*],
[edit logical-systems *logical-system-name* system syslog host],
[edit system syslog file *filename*],
[edit system syslog host]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Record the priority (facility and severity level) in each standard-format system log message directed to a file or remote destination.

When the **structured-data** statement is also included at the **[edit system syslog file *filename*]** hierarchy level, this statement is ignored for the file.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Including Priority Information in System Log Messages on page 21
- System Log Explorer
- **structured-data on page 138**

facility-override (Security)

Syntax

```
facility-override facility;
```

Hierarchy Level

[edit security log]

Release Information

Statement introduced in Junos OS Release 12.3X48-D35 for SRX Series devices.

Description

Alternate facility for logging to remote host.

System log server is set up to use a facility-override value to filter or write log files received by a system log agent.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

file (Security Log)

Syntax

```
file {
   files max-file-number;
   name file-name;
   path binary-log-file-path;
   size maximum-file-size;
}
```

Hierarchy Level

[edit security log]

Release Information

Statement modified in Junos OS Release 9.2.

Description

Configure security log file options for logs in binary format.

Options

- **files *number***—Specify the maximum number of binary log files.

Range: 2 through 10 files.

- **name *name*** —Name of the file to log messages.
- **path *filepath***—Specify the path of the binary log file.
- **size *maximum-file-size***—Maximum size of each trace file, in megabytes (MB).

Range: 1 KB through 10 MB

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- syslog (System) on page 139

file (System Logging)

Syntax

```
file filename {
  facility severity;
  archive {
    files number;
    size size;
    (no-world-readable | world-readable);
  }
  explicit-priority;
  match "regular-expression";
  match-string string-name;
  structured-data {
    brief;
  }
}
```

Hierarchy Level [edit system syslog]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the logging of system messages to a file.

Options *facility*—Class of messages to log. To specify multiple classes, include multiple ***facility severity*** statements. For a list of the facilities, see Table 3 on page 5.

file *filename*—File in the **/var/log** directory in which to log messages from the specified facility. To log messages to more than one file, include more than one **file** statement.

severity—Severity of the messages that belong to the facility specified by the paired ***facility*** name. Messages with severities of the specified level and higher are logged. For a list of the severities, see Table 4 on page 5.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Directing System Log Messages to a Log File on page 17
- *Junos OS System Log Reference for Security Devices*

files

Syntax

files *number*;

Hierarchy Level

[edit system syslog archive],
[edit system syslog file *filename* archive]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for EX Series switches.

Description

Configure the maximum number of archived log files to retain. When the Junos OS logging utility has written a defined maximum amount of data to a log file ***logfile***, it closes the file, compresses it, and renames it to ***logfile*.0.gz** (for information about the maximum file size, see size). The utility then opens and writes to a new file called ***logfile***. When the new file reaches the maximum size, the ***logfile*.0.gz** file is renamed to ***logfile*.1.gz**, and the new file is closed, compressed, and renamed ***logfile*.0.gz**. By default, the logging facility creates up to ten archive files in this manner. Once the maximum number of archive files exists, each time the active log file reaches the maximum size, the contents of the oldest archive file are lost (overwritten by the next oldest file).

Options

number—Maximum number of archived files.

Range: 1 through 1000

Default: 10 files

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Junos OS System Log Reference for Security Devices*
- size on page 137

host (Security Log)

Syntax

```
host {
  ip-address;
  port port-number;
}
```

Hierarchy Level [edit security log stream *stream-name*]

Release Information Statement introduced in Junos OS Release 9.2.

Description You can specify the IP address of the server to which the security logs are streamed.

Options

- *ip-address*—Specify IP address of the host.
- **port** *port-number*—Specify host port number.

Default: The default destination port is the system log port. For UDP or TCP, the default port is 514. For TLS, the default port is 6514.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- syslog (System) on page 139

limit (Security Log)

Syntax limit *value*;

Hierarchy Level [edit security log cache]

Release Information Statement modified in Junos OS Release 9.2.

Description Specify the number of security log entries to be kept in memory.

Options Once the maximum value limit is reached, new entries will not be added until the cache size drops.

Range: 0 through 4,294,967,295

Default: 10,000 security log entries.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- syslog (System) on page 139

log (Security)

Syntax

```
log {
  cache {
    exclude exclude-name {
      destination-address destination-address;
      destination-port destination-port;
      event-id event-id;
      failure;
      interface-name interface-name;
      policy-name policy-name;
      process process-name;
      protocol protocol;
      source-address source-address;
      source-port source-port;
      success;
      user-name user-name;
    }
    limit value;
  }
  disable;
  event-rate rate;
  facility-override (authorization | daemon | ftp | kernel | local | user);
  file {
    files max-file-number;
    name file-name;
    path binary-log-file-path;
    size maximum-file-size;
  }
  format (binary | sd-syslog | syslog);
  max-database-record <max-database-record>;
  mode (event | stream);
  rate-cap <rate-cap-value>;
  report;
  (source-address source-address | source-interface interface-name);
  stream stream-name {
    category (all | content-security | fw-auth | screen | alg | nat | flow | sctp | gtp | ipsec | idp
      | rtlog |pst-ds-lite | appqos |secintel);
    file {
      name file-name;
      size file-size;
      rotation max-rotation-number;
    }
    filter {
      threat-attack;
      }
    format (binary | sd-syslog | syslog | welf);
    host {
      ip-address;
      port port-number;
    }
    rate-limit {
      log-rate;
    }
    severity (alert | critical | debug | emergency | error | info | notice | warning);
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (world-readable | no-world-readable);
    }
    flag (all | configuration | hpl | report | source);
    no-remote-trace;
  }
  transport {
    protocol (udp | tcp | tls);
    tcp-connections tcp-connections;
    tls-profile tls-profile-name;
  }
  utc-timestamp;
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 9.2.

Description Configure security log. Set the mode of logging (event for traditional system logging or stream for streaming security logs through a revenue port to a server). You can also specify all the other parameters for security logging.

On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the default mode supported for collecting/saving traffic logs is the event mode (on-box). Data plane events are written to system log files in a similar manner to control plane events. To specify binary format for the security logs, see “Configuring On-Box Binary Security Log Files” on page 93.

On SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices, the default and recommend mode that is supported for collecting/saving traffic logs is the stream mode (off-box). The system streams already-processed data plane events directly to external log servers, bypassing the Routing Engine. To specify binary format and an external server, see “Configuring Off-Box Binary Security Log Files” on page 95.

Options

cache—Cache security log events in the audit log buffer.

disable—Disable the security logging for the device.

event-rate ***rate***—Limit the rate at which logs are streamed per second.

Range: 0 through 1500

Default: 1500

facility-override—Alternate facility for logging to remote host.

file—Specify the security log file options for logs in binary format.

Values:

- ***max-file-number***—Maximum number of binary log files.
  - The range is 2 through 10 and the default value is 10.
- ***file-name***—Name of binary log file.
- ***binary-log-file-path***—Path to binary log files.
- ***maximum-file-size***—Maximum size of binary log file in megabytes.
  - The range is 1 through 10 and the default value is 10.

format—Set the security log format for the device.

max-database-record—The following are the disk usage range limits for the database:

Range:

- SRX1500, SRX4100, and SRX4200: 0 through 15,000,000
- vSRX: 0 through 1,000,000

Default:

- SRX1500, SRX4100, and SRX4200: 15,000,000
- vSRX: 1,000,000

NOTE: Be sure there is enough free space in /var/log/hostlogs/, otherwise logs might be dropped when written into the database.

mode—Control how security logs are processed and exported.

rate-cap ***rate-cap-value***—Work with event mode only. This option limits the rate at which data plane logs are generated per second.

Range: 0 through 5000 logs per second

Default: 5000 logs per second

source-address ***source-address***—Specify a source IP address or IP address used when exporting security logs, which is mandatory to configure *stream host*.

source-interface *interface-name*—Specify a source interface name, which is mandatory to configure *stream host*.

NOTE: **The source-address and source-interface** are alternate values. Using one of the options is mandatory.

stream—Every stream can configure file or host.

- ***category***— Type of events that might be logged.
- ***file name***—Specify the filename.
- ***file size***—Specify the file size.
  - SRX1500, SRX4100, and SRX4200—The default value is 25 MB and the range is 10 MB through 50 MB.
  - vSRX - The default value is 2 MB and the range is 1 MB through 3 MB.
- ***rotation***—Configure the maximum file number for rotation.
  - The default value is 10 and the range is 2 through 19.
- ***rate-limit***—Rate-limit for security logs.
  - The range is 1 through 65,535 logs per second and the default value is 65,535 .
- ***filter***—Selects the filter to filter the logs to be logged.
- ***format***—Specify the log stream format.
- ***host***—Destination to send security logs.
- ***severity***—Severity threshold for security logs.

traceoptions—Specify security log daemon trace options.

transport—Set security log transport settings.

utc-timestamp—Specify to use UTC time for security log timestamps.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

log (Services)

Syntax

```
log {
  all;
  errors;
  info;
  sessions-allowed;
  sessions-dropped;
  sessions-ignored;
  sessions-whitelisted;
  warning;
}
```

Hierarchy Level [edit services ssl proxy profile *profile-name* actions]

Release Information Statement introduced in Junos OS Release 12.1X44-D10.

Description Specify the logging actions.

Options

- **all**—Log all events.
- **errors**—Log all error events.
- **info**—Log all information events.
- **sessions-allowed**—Log SSL session allowed events after an error.
- **sessions-dropped**—Log only SSL session dropped events.
- **sessions-ignored**—Log session ignored events.
- **sessions-whitelisted**—Log SSL session whitelisted events.
- **warning**—Log all warning events.

Required Privilege Level services—To view this statement in the configuration.
services-control—To add this statement to the configuration.

Related Documentation

- *Configuring SSL Proxy*

log-prefix (System)

Syntax log-prefix *string*;

Hierarchy Level [edit system syslog host]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Include a text string in each message directed to a remote destination.

Options ***string***—Text string to include in each message.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Adding a Text String to System Log Messages Directed to a Remote Destination on page 33
- *Junos OS System Log Reference for Security Devices*

log-rotate-frequency

Syntax log-rotate-frequency *frequency*;

Hierarchy Level [set system syslog]

Release Information Statement introduced in Junos OS Release 11.3.

Description Configure the system log file rotation frequency by configuring the time interval for checking the log file size.

When the log file size has exceeded the configured limit, the old log file is archived and a new log file is created.

Options ***frequency***—Frequency of rotation of the system log file.

Range: 1 minute through 59 minutes

Default: 15 minutes

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Specifying Log File Size, Number, and Archiving Properties on page 19
- **syslog on page 139**

match

Syntax

match "*regular-expression*";

Hierarchy Level

[edit logical-systems *logical-system-name* system syslog file *filename*],
[edit logical-systems *logical-system-name* system syslog user (*username* | *)],
[edit system syslog file *filename*],
[edit system syslog host *hostname* | other-routing-engine| scc-master)],
[edit system syslog user (*username* | *)]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Specify a text string that must (or must not) appear in a message for the message to be logged to a destination.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Using Regular Expressions to Refine the Set of Logged Messages on page 25
- **match-string on page 128**

match-string

Syntax match-string [*string-name*];

Hierarchy Level [edit system syslog file *filename*],
[edit system syslog host *hostname*],
[edit system syslog user *username*]

Release Information Statement introduced in Junos OS Release 16.1.

Description Specify a text substring that must appear in a message that is logged to a destination. The statement reduces the CPU utilization while displaying the system log messages.

The **match-string** configuration statement can be configured along with the **match** configuration statement. When you configure both **match** and **match-string**, the conditions set for a particular substring in the **match-string** configuration statement is read first. If the conditions in the **match-string** configuration statement are not satisfied, then the conditions set in the **match** configuration statements is executed.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Using Regular Expressions to Refine the Set of Logged Messages on page 25

mode (Security Log)

Syntax mode (event | stream)

Hierarchy Level [edit security log]

Release Information Statement introduced in Junos OS Release 10.0.

Description Set the mode of logging (event for traditional system logging or stream for streaming security logs through a revenue port to a server).

Options

- **event**— Process security logs in the control plane.
- **stream**—Process security logs directly in the forwarding plane.

Default:

- event is a default mode on SRX100, SRX110, SRX210, SRX220, SRX240, SRX300, SRX320, SRX340, SRX345, SRX550, SRX550M, SRX650, and SRX1500 devices.
- stream is a default mode on SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800, SRX4100, and SRX4200 devices.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- syslog (System) on page 139

no-remote-trace (System)

Syntax no-remote-trace;

Hierarchy Level [edit system scripts commit traceoptions]

Release Information Statement introduced in Junos OS Release 11.2.

Description Disable remote tracing.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *traceoptions (Security Datapath Debug)*

pic-services-logging

Syntax

```
pic-services-logging {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
```

Hierarchy Level [edit system processes]

Release Information Statement introduced in Junos OS Release 8.5.

Description Enable PICs to send special logging information to the Routing Engine for archiving on a hard disk.

Options

- **command** ***binary-file-path***—Path to the binary process.
- **disable**—Disable the PIC services logging process.
- **failover**—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.
  - **alternate-media**—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.
  - **other-routing-engine**—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, the device reboots from the secondary Routing Engine.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- syslog (System) on page 139

port (Syslog)

Syntax port *port number*;

Hierarchy Level [edit system syslog host *hostname* | other-routing-engine| scc-master)]

Release Information Statement introduced in Junos OS Release 11.3.

Description Specify the port number for the remote syslog server.

Options *port number*—Port number of the remote syslog server.

Range: 0 through 65535

Default: 514

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- syslog on page 139
- *host*

rate-cap

Syntax

```
rate-cap <rate-cap-value>;
```

Hierarchy Level

```
[edit security log]
```

Release Information

Statement introduced in Junos OS Release 10.0.

Description

Limits the rate at which data plane logs will be generated per second.

On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the default mode supported for collecting/saving traffic logs is the event mode (on-box). Data plane events are written to system log files in a similar manner to control plane events. To specify binary format for the security logs, see “Configuring On-Box Binary Security Log Files” on page 93.

Options

rate-cap *rate-cap-value*—Works with event mode only. Limits the rate at which data plane logs will be generated per second

Range: 0 through 5000 logs per second

Default: 5000 logs per second

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- syslog (System) on page 139

report (Security Log)

Syntax report;

Hierarchy Level [edit security log (Security)]

Release Information Statement introduced in Junos OS Release 15.1X49-D100

Description Set security log report settings.

On-box reporting offers a comprehensive reporting facility where your security management team can spot a security event when it occurs, immediately access and review pertinent details about the event, and quickly decide appropriate remedial action.

The on-box reporting feature is enabled by default on a SRX Series device with Junos OS Release 15.1X49-D100 or later.

If you are upgrading your SRX Series device from a Junos OS Release prior to Junos OS 15.1X49-D100, then on-box reporting feature is disabled by default. You need to run the **set security log report** command to enable the on-box reporting feature on the device.

Options **report**—Enable log report.

Required Privilege Level *[none specified]*
The remaining statements are explained separately. See CLI Explorer.

Related Documentation

- log (Security) on page 120

security-log

Syntax

```
security-log {
   command binary-file-path;
   disable;
   failover (alternate-media | other-routing-engine);
}
```

Hierarchy Level [edit system processes]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the security log process.

Options

- **command** ***binary-file-path***—Path to the binary process.
- **disable**—Disable the security log process.
- **failover**—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.
  - **alternate-media**—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.
  - **other-routing-engine**—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- syslog (System) on page 139

security-log-percent-full

Syntax security-log-percent-full *percentage*;

Hierarchy Level [edit security alarms potential-violation]

Release Information Statement introduced in Junos OS Release 11.2.

Description Raise a security alarm when security log exceeds a specified percent of total capacity.

Options ***percentage***—Percentage of security log capacity at which a security alarm is raised.

Range: 0 through 100 percent

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- syslog (System) on page 139

severity (Security Log)

Syntax severity (alert | critical | debug | emergency | error | info | notice | warning)

Hierarchy Level [edit security log stream *stream-name*]

Release Information Statement modified in Junos OS Release 9.2.

Description Set severity threshold for security logs.

Options

- **alert**— Conditions that require immediate attention.
- **critical**—Critical conditions.
- **debug**—Information normally used in debugging.
- **emergency**—Conditions that cause security functions to stop.
- **error**—General error conditions.
- **info**—Information about normal security operations.
- **notice**—Nonerror conditions that are of interest.
- **warning**—General warning conditions.

Default: debug.

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

- syslog (System) on page 139

size (System)

Syntax

size *size*;

Hierarchy Level

[edit system syslog archive],
[edit system syslog file *filename* archive]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the maximum amount of data that the Junos OS logging utility writes to a log file ***logfile*** before archiving it (closing it, compressing it, and changing its name to ***logfile*.0.gz**). The utility then opens and writes to a new file called ***logfile***. For information about the number of archive files that the utility creates in this way, see files.

Options

size—Maximum size of each system log file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).

Syntax: ***x*k** to specify the number of kilobytes, ***x*m** for the number of megabytes, or ***x*g** for the number of gigabytes

Range: 64 KB through 1 GB

Default: 1 MB for MX Series routers the QFX Series, and the OCX Series

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Specifying Log File Size, Number, and Archiving Properties on page 19
- System Log Explorer
- files on page 117

structured-data

Syntax

```
structured-data {
  brief;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* system syslog file *filename*],
[edit system syslog file *filename*]

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Write system log messages to the log file in structured-data format, which complies with Internet draft draft-ietf-syslog-protocol-23, *The syslog Protocol* (http://tools.ietf.org/html/draft-ietf-syslog-protocol-23).

NOTE: When this statement is included, other statements that specify the format for messages written to the file are ignored (the **explicit-priority** statement at the **[edit system syslog file *filename*]** hierarchy level and the **time-format** statement at the **[edit system syslog]** hierarchy level).

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Logging Messages in Structured-Data Format on page 18
- *Junos OS System Log Reference for Security Devices*
- **explicit-priority on page 114**
- **time-format on page 142**

syslog (System)

Syntax

```
syslog {
  allow-duplicates;
  archive {
    (binary-data| no-binary-data);
    files number;
    size maximum-file-size;
    start-time "YYYY-MM-DD.hh:mm";
    transfer-interval minutes;
    (world-readable | no-world-readable);
  }
  console {
    facility severity;
  }
  file filename {
    facility severity;
    explicit-priority;
    match "regular-expression";
    archive {
      (binary-data| no-binary-data);
      files number;
      size maximum-file-size;
      start-time "YYYY-MM-DD.hh:mm";
      transfer-interval minutes;
      (world-readable | no-world-readable);
    }
    structured-data {
      brief;
    }
  }
  host (hostname | other-routing-engine | scc-master) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
    source-address source-address;
    structured-data {
      brief;
    }
    port port number;
  }
  log-rotate-frequency frequency;
  server {
    routing-instances (routing-instance-name | all | default) {
      disable;
  source-address source-address;
  time-format(millisecond | year | year millisecond);
  user (username | *) {
    facility severity;
    match "regular-expression";
  }
}
```

Hierarchy Level

[edit system]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the types of system log messages to send to files, to a remote destination, to user terminals, or to the system console.

The remaining statements are explained separately.

Options

archive—Define parameters for archiving log messages.

console—Send log messages of a specified class and severity to the console.

file—Send log messages to a named file.

host —Remote location to be notified of specific log messages.

log-rotate-frequency—Configure the interval for checking logfile size and archiving messages.

server—Enable a syslog server for compute nodes and VMs in an App Engine.

source-address—Include a specified address as the source address for log messages.

time-format—Additional information to include in the system log time stamp.

user—Notify a specific user of the log event.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Junos OS System Log Overview on page 3
- System Log Explorer

system

Syntax system { ... }

Hierarchy Level [edit]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure system management properties.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *System Management Configuration Statements*

time-format

Syntax time-format (year | millisecond | year millisecond);

Hierarchy Level [edit system syslog]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Include the year, the millisecond, or both, in the timestamp on every standard-format system log message. The additional information is included for messages directed to each destination configured by a **file**, **console**, or **user** statement at the **[edit system syslog]** hierarchy level, but not to destinations configured by a **host** statement.

NOTE: By default, in a FreeBSD console, the additional time information is not available in system log messages directed to each destination configured by a **host** statement. However, in a Junos OS specific implementation using the FreeBSD console, the additional time information is available in system log messages directed to each destination.

By default, the timestamp specifies the month, date, hour, minute, and second when the message was logged—for example, **Aug 21 12:36:30**. However, the timestamp for traceoption messages is specified in milliseconds by default, and is independent of the **[edit system syslog time-format]** statement.

NOTE: When the **structured-data** statement is included at the **[edit system syslog file *filename*]** hierarchy level, this statement is ignored for the file.

Options **millisecond**—Include the millisecond in the timestamp.

year—Include the year in the timestamp.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Including the Year or Millisecond in Timestamps on page 24
- *Junos OS System Log Reference for Security Devices*
- **structured-data on page 138**

traceoptions (Security Log)

Syntax

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag (all | configuration | hpl | report | source);
  no-remote-trace;
}
```

Hierarchy Level [edit security log]

Release Information Statement modified in Junos OS Release 9.2.

Description Configure security log tracing options.

Options

- **file**—Configure the trace file options.
  - ***filename***—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. By default, the name of the file is the name of the process being traced.
  - **files *number***—Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed to ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  - **match *regular-expression***—Refine the output to include lines that contain the regular expression.
  - **size *maximum-file-size***—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the **trace-file** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

    If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and a filename.

    Syntax: ***x* K** to specify KB, ***x* m** to specify MB, or ***x* g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

  - **world-readable** | **no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace with all flags enabled
  - **configuration**—Trace configuration events
  - **hpl**— Trace HPL logging
  - **report**— Trace report
  - **source**—Communicate with security log forwarder
- **no-remote-trace**—Set remote tracing as disabled.

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- syslog (System) on page 139

tracing

Syntax

```
tracing {
  destination-override syslog host ip-address;
}
```

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 9.2.

Description Configure the router to enable remote tracing to a specified host IP address. The default setting is disabled.

The following processes are supported:

- chassisd—Chassis-control process
- eventd—Event-processing process
- cosd—Class-of-service process
- spd—Adaptive-services process

You can use the **no-remote-trace** statement, under the **[edit system process-name traceoptions]** hierarchy, to disable remote tracing.

Options **destination-override syslog host *ip-address***—Overrides the global config under **system tracing** and has no effect if **system tracing** is not configured.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Junos OS Tracing and Logging Operations*
- destination-override on page 111
- *no-remote-trace*

user (System Logging)

Syntax

```
user (username | *) {
  facility severity;
  match "regular-expression";
  match-string string-name;
}
```

Hierarchy Level

[edit system syslog]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure the logging of system messages to user terminals.

Options

***** (the asterisk)—Log messages to the terminal sessions of all users who are currently logged in.

facility—Class of messages to log. To specify multiple classes, include multiple ***facility severity*** statements. For a list of the facilities, see Table 3 on page 5.

severity—Severity of the messages that belong to the facility specified by the paired ***facility*** name. Messages with severities the specified level and higher are logged. For a list of the severities, see Table 4 on page 5.

username—Junos OS login name of the user whose terminal session is to receive system log messages. To log messages to more than one user's terminal session, include more than one **user** statement.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Directing System Log Messages to a User Terminal on page 18
- Junos OS System Logging Facilities and Message Severity Levels on page 4
- *Junos OS System Log Reference for Security Devices*

world-readable

Syntax

world-readable | no-world-readable;

Hierarchy Level

[edit system syslog archive],
[edit system syslog file *filename* archive]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Grant all users permission to read log files, or restrict the permission only to the **root** user and users who have the Junos OS **maintenance** permission.

Default

no-world-readable

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Specifying Log File Size, Number, and Archiving Properties on page 19
- *Junos OS System Log Reference for Security Devices*

Operational Commands

- clear log
- clear security log
- clear security log file
- clear security log stream file
- monitor list
- monitor start
- monitor stop
- show log
- show security log
- show security log file
- show security log severity
- show security log query

clear log

Syntax

```
clear log filename
<all>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description

Remove contents of a log file.

Options

filename—Name of the specific log file to delete.

all—(Optional) Delete the specified log file and all archived versions of it.

Required Privilege Level

clear

Related Documentation

- show log on page 158

List of Sample Output

clear log on page 148

Output Fields

See *file list* for an explanation of output fields.

Sample Output

clear log

The following sample commands list log file information, clear the contents of a log file, and then display the updated log file information:

```
user@host> file list lcc0-re0:/var/log/sampled detail
lcc0-re0:
--------------------------------------------------------------------------
-rw-r-----  1 root  wheel      26450 Jun 23 18:47 /var/log/sampled
total 1

user@host> clear log lcc0-re0:sampled
lcc0-re0:
--------------------------------------------------------------------------

user@host> file list lcc0-re0:/var/log/sampled detail
lcc0-re0:
--------------------------------------------------------------------------
-rw-r-----  1 root  wheel         57 Sep 15 03:44 /var/log/sampled
total 1
```

clear security log

Syntax

```
clear security log
<all>
<destination-address>
<destination-port>
<event-id>
<failure>
<interface-name>
<newer-than>
<older--than>
<process>
<protocol>
<report>
<severity>
<source-address>
<source-port>
<success>
<username>
```

Release Information Command introduced in Junos OS Release 11.2.

Description Delete the event log.

Options

all—Clear all audit event logs stored in the device memory.

destination-address—Clear audit event logs with the specified destination address.

destination-port—Clear audit event logs with the specified destination port.

event-id—Clear audit event logs with the specified event identification number.

failure—Clear failed audit event logs.

interface-name—Clear audit event logs with the specified interface.

newer-than—Clear audit event logs newer than the specified date and time.

older-than—Clear audit event logs older than the specified date and time

process—Clear audit event logs with the specified process that generated the event.

protocol—Clear audit event logs generated through the specified protocol.

report—Clear on-box reports for system traffic logs.

severity—Clear audit event logs generated with the specified severity.

source-address—Clear audit event logs with the specified source address.

source-port—Clear audit event logs with the specified source port.

success—Clear successful audit event logs.

username—Clear audit event logs generated for the specified user.

Required Privilege Level clear

Related Documentation

- exclude (Security Log) on page 113
- show security log on page 162

Sample Output

clear security log all

```
user@host> clear security log all
7905 security log events cleared
```

clear security log file

Syntax clear security log file

Release Information Command introduced in Junos OS Release 12.1.

Description Deletes the content of an event mode security log file stored on the device in binary format.

Required Privilege Level clear

Related Documentation

- show security log file on page 165

Sample Output

clear security log file

```
user@host> clear security log file
7905 security log events cleared
```

clear security log stream file

Syntax

```
clear security log query
clear security log stream
file <file-name>
```

Release Information

Command introduced in Junos OS Release 15.1X49-D70 for SRX1500, SRX4100, and SRX4200 Series devices and vSRX instances.

Description

- **clear security log query**—Clear the content of the database.
- **clear security log stream file**—Clear the content of the current log file.

Required Privilege Level

clear

Output Fields

The following outputs are occurred in two conditions:

- Clear log stream file successfully, when there is log file.
- Clear log stream file error or does not exits, when there is no log file.

monitor list

Syntax monitor list

Release Information Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description Display the status of monitored log and trace files.

Options This command has no options.

Additional Information Log files are generated by the routing protocol process or by system logging. The log files generated by system logging are configured with the **syslog** statement at the **[edit system]** hierarchy level and the **options** statement at the **[edit routing-options]** hierarchy level. The trace files generated by the routing protocol process are those configured with **traceoptions** statements at the **[edit routing-options]**, **[edit interfaces]**, and **[edit protocols *protocol*]** hierarchy levels.

Required Privilege Level trace

Related Documentation

- monitor start on page 155
- monitor stop on page 157

List of Sample Output monitor list on page 153

Output Fields Table 32 on page 153 describes the output fields for the **monitor list** command. Output fields are listed in the approximate order in which they appear.

Table 32: monitor list Output Fields

Field Name	Field Description
monitor start	Indicates the file is being monitored.
"*filename*"	Name of the file that is being monitored.
Last changed	Date and time at which the file was last modified.

Sample Output

monitor list

```
user@host> monitor list
monitor start "vrrpd" (Last changed Dec 03:11:06 20)
monitor start "cli-commands" (Last changed Nov 07:3)
```

monitor start

Syntax monitor start *filename*

Release Information Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description Start displaying the system log or trace file and additional entries being added to those files.

Options *filename*—Specific log or trace file.

Additional Information Log files are generated by the routing protocol process or by system logging. The log files generated by system logging are configured with the **syslog** statement at the **[edit system]** hierarchy level and the **options** statement at the **[edit routing-options]** hierarchy level. The trace files generated by the routing protocol process are configured with **traceoptions** statements at the **[edit routing-options]**, **[edit interfaces]**, and **[edit protocols *protocol*]** hierarchy levels.

NOTE: To monitor a log file within a logical system, issue the **monitor start** ***logical-system-name/filename*** command.

Required Privilege Level trace

Related Documentation

- monitor list on page 153
- monitor stop on page 157

List of Sample Output monitor start on page 156

Output Fields Table 33 on page 155 describes the output fields for the **monitor start** command. Output fields are listed in the approximate order in which they appear.

Table 33: monitor start Output Fields

Field Name	Field Description
****filename* ***	Name of the file from which entries are being displayed. This line is displayed initially and when the command switches between log files.
Date and time	Timestamp for the log entry.

Sample Output

monitor start

```
user@host> monitor start system-log
*** system-log***
Jul 20 15:07:34 hang sshd[5845]: log: Generating 768 bit RSA key.
Jul 20 15:07:35 hang sshd[5845]: log: RSA key generation complete.
Jul 20 15:07:35 hang sshd[5845]: log: Connection from 204.69.248.180 port 912
Jul 20 15:07:37 hang sshd[5845]: log: RSA authentication for root accepted.
Jul 20 15:07:37 hang sshd[5845]: log: ROOT LOGIN as 'root' from host.example.com
Jul 20 15:07:37 hang sshd[5845]: log: Closing connection to 204.69.248.180
```

monitor stop

Syntax

monitor stop *filename*

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Stop displaying the system log or trace file.

Options

filename—Specific log or trace file.

Additional Information

Log files are generated by the routing protocol process or by system logging. The log files generated by system logging are those configured with the **syslog** statement at the **[edit system]** hierarchy level and the **options** statement at the **[edit routing-options]** hierarchy level. The trace files generated by the routing protocol process are those configured with **traceoptions** statements at the **[edit routing-options]**, **[edit interfaces]**, and **[edit protocols *protocol*]** hierarchy levels.

Required Privilege Level

trace

Related Documentation

- monitor list on page 153
- monitor start on page 155

List of Sample Output

monitor stop on page 157

Output Fields

This command produces no output.

Sample Output

monitor stop

```
user@host> monitor stop
```

show log

List of Syntax

Syntax on page 158
Syntax (QFX Series and OCX Series) on page 158
Syntax (TX Matrix Router) on page 158

Syntax

```
show log
<filename | user <username>>
```

Syntax (QFX Series and OCX Series)

```
show log filename
<device-type (device-id | device-alias)>
```

Syntax (TX Matrix Router)

```
show log
<all-lcc | lcc number | scc>
<filename | user <username>>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Option *device-type (device-id* | *device-alias*) is introduced in Junos OS Release 13.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

List log files, display log file contents, or display information about users who have logged in to the router or switch.

NOTE: On MX Series routers, modifying a configuration to replace a service interface with another service interface is treated as a catastrophic event. When you modify a configuration, the entire configuration associated with the service interface—including NAT pools, rules, and service sets—is deleted and then re-created for the newly specified service interface. If there are active sessions associated with the service interface that is being replaced, these sessions are deleted and the NAT pools are then released, which leads to the generation of the NAT_POOL_RELEASE system log messages. However, because NAT pools are already deleted as a result of the catastrophic configuration change and no longer exist, the NAT_POOL_RELEASE system log messages are not generated for the changed configuration.

Options

none—List all log files.

<all-lcc | lcc *number* | scc>—(Routing matrix only)(Optional) Display logging information about all T640 routers (or line-card chassis) or a specific T640 router (replace ***number*** with a value from 0 through 3) connected to a TX Matrix router. Or, display logging information about the TX Matrix router (or switch-card chassis).

device-type—(QFabric system only) (Optional) Display log messages for only one of the following device types:

- **director-device**—Display logs for Director devices.
- **infrastructure-device**—Display logs for the logical components of the QFabric system infrastructure, including the diagnostic Routing Engine, fabric control Routing Engine, fabric manager Routing Engine, and the default network Node group and its backup (NW-NG-0 and NW-NG-0-backup).
- **interconnect-device**—Display logs for Interconnect devices.
- **node-device**—Display logs for Node devices.

NOTE: If you specify the **device-type** optional parameter, you must also specify either the **device-id** or **device-alias** optional parameter.

(*device-id* | *device-alias*)—If a device type is specified, display logs for a device of that type. Specify either the device ID or the device alias (if configured).

filename—(Optional) Display the log messages in the specified log file. For the routing matrix, the filename must include the chassis information.

NOTE: The *filename* parameter is mandatory for the QFabric system. If you did not configure a syslog filename, specify the default filename of **messages**.

user <*username*>—(Optional) Display logging information about users who have recently logged in to the router or switch. If you include ***username***, display logging information about the specified user.

Required Privilege Level trace

Related Documentation

- syslog (System) on page 139

List of Sample Output

show log on page 159
show log filename on page 160
show log filename (QFabric System) on page 160
show log user on page 161

Sample Output

show log

```
user@host> show log
```

```
total 57518
-rw-r--r--  1 root  bin      211663 Oct  1 19:44 dcd
-rw-r--r--  1 root  bin      999947 Oct  1 19:41 dcd.0
-rw-r--r--  1 root  bin      999994 Oct  1 17:48 dcd.1
-rw-r--r--  1 root  bin      238815 Oct  1 19:44 rpd
-rw-r--r--  1 root  bin     1049098 Oct  1 18:00 rpd.0
-rw-r--r--  1 root  bin     1061095 Oct  1 12:13 rpd.1
-rw-r--r--  1 root  bin     1052026 Oct  1 06:08 rpd.2
-rw-r--r--  1 root  bin     1056309 Sep 30 18:21 rpd.3
-rw-r--r--  1 root  bin     1056371 Sep 30 14:36 rpd.4
-rw-r--r--  1 root  bin     1056301 Sep 30 10:50 rpd.5
-rw-r--r--  1 root  bin     1056350 Sep 30 07:04 rpd.6
-rw-r--r--  1 root  bin     1048876 Sep 30 03:21 rpd.7
-rw-rw-r--  1 root  bin       19656 Oct  1 19:37 wtmp
```

show log filename

```
user@host> show log rpd
Oct  1 18:00:18 trace_on: Tracing to ?/var/log/rpd? started
Oct  1 18:00:18 EVENT <MTU> ds-5/2/0.0 index 24 <Broadcast PointToPoint Multicast
Oct  1 18:00:18
Oct  1 18:00:19 KRT recv len 56 V9 seq 148 op add Type route/if af 2 addr
192.0.2.21 nhop type local nhop 192.0.2.21
Oct  1 18:00:19 KRT recv len 56 V9 seq 149 op add Type route/if af 2 addr
192.0.2.22 nhop type unicast nhop 192.0.2.22
Oct  1 18:00:19 KRT recv len 48 V9 seq 150 op add Type ifaddr index 24 devindex
43
Oct  1 18:00:19 KRT recv len 144 V9 seq 151 op chnge Type ifdev devindex 44
Oct  1 18:00:19 KRT recv len 144 V9 seq 152 op chnge Type ifdev devindex 45
Oct  1 18:00:19 KRT recv len 144 V9 seq 153 op chnge Type ifdev devindex 46
Oct  1 18:00:19 KRT recv len 1272 V9 seq 154 op chnge Type ifdev devindex 47
...
```

show log filename (QFabric System)

```
user@qfabric> show log messages
Mar 28 18:00:06 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:06 ED1486
 chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 1, jnxFruL3Index 0,
jnxFruName PIC: 48x 10G-SFP+ @ 0/0/*, jnxFruType 11, jnxFruSlot 0,
jnxFruOfflineReason 2, jnxFruLastPowerOff 0, jnxFruLastPowerOn 2159)
Mar 28 18:00:07 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:07 ED1486
 chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 2, jnxFruL3Index 0,
jnxFruName PIC:  @ 0/1/*, jnxFruType 11, jnxFruSlot 0, jnxFruOfflineReason 2,
jnxFruLastPowerOff 0, jnxFruLastPowerOn 2191)
Mar 28 18:00:07 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:07 ED1492
 chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 1, jnxFruL3Index 0,
jnxFruName PIC: 48x 10G-SFP+ @ 0/0/*, jnxFruType 11, jnxFruSlot 0,
jnxFruOfflineReason 2, jnxFruLastPowerOff 0, jnxFruLastPowerOn 242726)
Mar 28 18:00:07 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:07 ED1492
 chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 2, jnxFruL3Index 0,
jnxFruName PIC:  @ 0/1/*, jnxFruType 11, jnxFruSlot 0, jnxFruOfflineReason 2,
jnxFruLastPowerOff 0, jnxFruLastPowerOn 242757)
Mar 28 18:00:16 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:16 ED1486
file: UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
Mar 28 18:00:27 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:27 ED1486
file: UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
```

```
Mar 28 18:00:50 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:50
_DCF_default___NW-INE-0_RE0_ file: UI_COMMIT: User 'root' requested 'commit'
operation (comment: none)
Mar 28 18:00:50 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:50
_DCF_default___NW-INE-0_RE0_ file: UI_COMMIT: User 'root' requested 'commit'
operation (comment: none)
Mar 28 18:00:55 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:55 ED1492
file: UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
Mar 28 18:01:10 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:01:10 ED1492
file: UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
Mar 28 18:02:37 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:02:37 ED1491
 chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 1, jnxFruL3Index 0,
jnxFruName PIC: 48x 10G-SFP+ @ 0/0/*, jnxFruType 11, jnxFruSlot 0,
jnxFruOfflineReason 2, jnxFruLastPowerOff 0, jnxFruLastPowerOn 33809)
```

show log user

```
user@host> show log user
usera    mg2546                    Thu Oct  1 19:37   still logged in
usera    mg2529                    Thu Oct  1 19:08 - 19:36  (00:28)
usera    mg2518                    Thu Oct  1 18:53 - 18:58  (00:04)
root     mg1575                    Wed Sep 30 18:39 - 18:41  (00:02)
root     ttyp2    aaa.bbbb.com     Wed Sep 30 18:39 - 18:41  (00:02)
userb    ttyp1    192.0.2.0        Wed Sep 30 01:03 - 01:22  (00:19)
```

show security log

Syntax

show security log {*all*| *destination-address*| *destination-port*| *event-id*| *failure*|*interface-name*| *newer-than*| *older-than*| *process*| *protocol*|*report*| *severity*| *sort-by*| *source-address*| *source-port*| *success*| *user*}

Release Information

Command introduced in Junos OS Release 11.2 .

Description

Display security event logs. This command continuously displays security events on the screen. To stop the display, press Ctrl+c.

Options

all—Display all audit event logs stored in the device memory.

destination-address—Display audit event logs with the specified destination address.

destination-port—Display audit event logs with the specified destination port.

event-id—Display audit event logs with the specified event identification number.

failure—Display failed audit event logs.

interface-name—Display audit event logs with the specified interface.

newer-than—Display audit event logs newer than the specified date and time.

older-than—Display audit event logs older than the specified date and time.

process—Display audit event logs with the specified process that generated the event.

protocol—Display audit event logs generated through the specified protocol.

report—Display on-box reports for system traffic logs.

severity—Display audit event logs generated with the specified severity.

sort-by—Display audit event logs generated sorted with the specified options.

source-address—Display audit event logs with the specified source address.

source-port—Display audit event logs with the specified source port.

success—Display successful audit event logs.

username—Display audit event logs generated for the specified user.

Required Privilege Level

view

Related Documentation

- exclude (Security Log) on page 113
- clear security log on page 149

List of Sample Output show security log on page 163

Output Fields Table 34 on page 163 lists the output fields for the **show security log** command. Output fields are listed in the approximate order in which they appear.

Table 34: show security log Output Fields

Field Name	Field Description
Event time	The timestamp of the events received. On SRX Series devices, security logs were always timestamped using the UTC time zone by running **set system time-zone utc** and **set security log utc-timestamp** CLI commands. Now, time zone can be defined using the local time zone by running the **set system time-zone time-zone** command to specify the local time zone that the system should use when timestamping the security logs.
Message	Security events are listed.

Sample Output

show security log

```
user@host> show security log
Event time               Message
2010-10-22 13:28:37 CST  session created 1.1.1.2/1-->2.2.2.2/1308
 icmp 1.1.1.2/1-->2.2.2.2/1308
 None None 1 policy1 trustZone untrustZone 52 N/A(N/A) ge-0/0/1.0
2010-10-22 13:28:38 CST  session created 1.1.1.2/1-->2.2.2.2/1308 icmp
1.1.1.2/1-->2.2.2.2/1308 None None 1 policy1 trustZone untrustZone 54 N/A(N/A)
ge-0/0/1.0

...

2010-10-22 13:36:12 CST  session denied m icmp 1(8) policy1 trustZone untrustZone
 N/A(N/A) ge-0/0/1.0
2010-10-22 13:36:14 CST  session denied 1.1.1.2/2-->2.2.2.2/54812  icmp 1(8)
policy1 trustZone untrustZone N/A(N/A) ge-0/0/1.0

...

2010-10-27 15:50:11 CST  IP spoofing! source: 2.2.2.20, destination: 2.2.2.2,
protocol-id: 17, zone name: trustZone, interface name: ge-0/0/1.0, action: drop
2010-10-27 15:50:11 CST  IP spoofing! source: source: 2.2.2.20, destination:
2.2.2.2, protocol-id: 17, zone name: trustZone, interface name: ge-0/0/1.0, action:
 drop

...

2011-02-18 15:53:34 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/certification-authority/ca-profile1-ca1.cert
2011-02-18 15:53:35 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/crl/ca-profile1.crl
2011-02-18 15:53:35 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/system-key-pair/system-generated.priv
2011-02-18 15:53:35 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/system-cert/system-generated.cert
2011-02-18 15:53:35 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/key-pair/cert1.priv
```

```
2011-02-18 15:53:42 CST  PKID_PV_OBJECT_READ: A PKI object was read into memory
from /var/db/certs/common/key-pair/test2.priv

...

2011-03-14 23:00:40 PDT  IDP_COMMIT_COMPLETED: IDP policy commit is complete.
                         IDP_POLICY_LOAD_FAILED: IDP policy loading failed ;poli
cy[/var/db/idpd/bins/.bin.gz.v], detector[/usr/libdata/libidp-detector.so.tgz.v]

 ,failure detail[Policy loading failed :: Policy file not found
2011-03-14 23:00:58 PDT  ]
                         IDP_POLICY_LOAD_FAILED: IDP policy loading failed ;poli
cy[/var/db/idpd/bins/.bin.gz.v], detector[/usr/libdata/libidp-detector.so.tgz.v]

 ,failure detail[Policy loading failed :: Policy file not found
2011-03-14 23:00:58 PDT  ]
                         IDP_POLICY_LOAD_FAILED: IDP policy loading failed ;poli
cy[/var/db/idpd/bins/.bin.gz.v], detector[/usr/libdata/libidp-detector.so.tgz.v]

 ,failure detail[Policy loading failed :: Policy file not found
2011-03-14 23:00:58 PDT  ]

...

Event time               Message
2011-03-21 14:21:49 CST  UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp
 9.9.9.1 source-address 6.6.6.1 '
2011-03-21 14:23:01 CST  UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp
 9.9.9.1 source-address 6.6.6.1 .5 '
2011-03-21 14:23:05 CST  KMD_PM_SA_ESTABLISHED: Local gateway: 7.7.7.1, Remote
gateway: 8.8.8.1, Local ID: ipv4(any:0,[0..3]=6.6.6.1), Remote ID:
ipv4(any:0,[0..3]=9.9.9.1), Direction: inbound, SPI: 37a2a179, AUX-SPI: 0, Mode:
 tunnel, Type: dynamic
2011-03-21 14:23:05 CST  KMD_PM_SA_ESTABLISHED: Local gateway: 7.7.7.1, Remote
gateway: 8.8.8.1, Local ID: ipv4(any:0,[0..3]=6.6.6.1), Remote ID:
ipv4(any:0,[0..3]=9.9.9.1), Direction: outbound, SPI: b2231c1f, AUX-SPI: 0, Mode:
 tunnel, Type: dynamic
2011-03-21 14:23:08 CST  UI_CMDLINE_READ_LINE: User 'root', command 'set date ntp
 9.9.9.1 source-address 6.6.6.1 '
2011-03-21 14:23:13 CST  UI_CMDLINE_READ_LINE: User 'root', command 'show security
 log '
```

show security log file

Syntax

show security log file

Release Information

Command introduced in Junos OS Release 12.1.

Description

Enables customers to view event-mode log files stored on the device in binary format.

On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the default mode supported for collecting/saving traffic logs is the event mode (on-box). Data plane events are written to system log files in a similar manner to control plane events. To specify binary format for the security logs, see “Configuring On-Box Binary Security Log Files” on page 93.

Required Privilege Level

view

Related Documentation

- show security log on page 162

List of Sample Output

show security log file on page 165

Output Fields

Table 35 on page 165 lists the output fields for the **show security log file** command. Output fields are listed in the approximate order in which they appear.

Table 35: show security log file Output Fields

Field Name	Field Description
Event time	The timestamp when the security event was received.
Message	The message describing the security event.

Sample Output

show security log file

```
user@host> show security log file
<14>1 2011-08-28T21:14:43 topstar RT_FLOW - RT_FLOW_SESSION_CREATE
[junos@2636.1.1.1.2.34 source-address="7.7.7.2" source-port="1"
destination-address="8.8.8.2" destination-port="5636" service-name="icmp"
nat-source-address="7.7.7.2" nat-source-port="1" nat-destination-address="8.8.8.2"
 nat-destination-port="5636" src-nat-rule-name="None" dst-nat-rule-name="None"
protocol-id="1" policy-name="client-to-server" source-zone-name="client"
destination-zone-name="server" session-id-32="60000442" username="N/A" roles="N/A"
 packet-incoming-interface="ge-0/0/0.0"]

<14>1 2011-08-28T21:14:45 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE
[junos@2636.1.1.1.2.34 reason="response received" source-address="7.7.7.2"
source-port="0" destination-address="8.8.8.2" destination-port="5636"
service-name="icmp" nat-source-address="7.7.7.2" nat-source-port="0"
nat-destination-address="8.8.8.2" nat-destination-port="5636"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="1"
policy-name="client-to-server" source-zone-name="client"
destination-zone-name="server" session-id-32="60000441" packets-from-client="1"
bytes-from-client="84" packets-from-server="1" bytes-from-server="84"
elapsed-time="3" application="UNKNOWN" nested-application="UNKNOWN" username="N/A"
 roles="N/A" packet-incoming-interface="ge-0/0/0.0"]

...

user@host> show security log file
<14>1 2011-11-17T23:41:46 topstar RT_FLOW - RT_FLOW_SESSION_CREATE_LS
[junos@2636.1.1.1.2.34 logical-system-name="LSYS1" source-address="3001::2"
source-port="0" destination-address="5001::2" destination-port="17420"
service-name="icmpv6" nat-source-address="3001::2" nat-source-port="0"
nat-destination-address="5001::2" nat-destination-port="17420"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218" username="N/A"
roles="N/A" packet-incoming-interface="ge-0/0/2.0"]


<14>1 2011-11-17T23:41:48 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE
[junos@2636.1.1.1.2.34 reason="response received" source-address="3001::2"
source-port="0" destination-address="5001::2" destination-port="17420"
service-name="icmpv6" nat-source-address="3001::2" nat-source-port="0"
nat-destination-address="5001::2" nat-destination-port="17420"
src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218"
packets-from-client="1" bytes-from-client="104" packets-from-server="1"
bytes-from-server="104" elapsed-time="3" application="UNKNOWN"
nested-application="UNKNOWN" username="N/A" roles="N/A"
packet-incoming-interface="ge-0/0/2.0" encrypted="No "]


<14>1 2011-11-17T23:41:48 topstar RT_FLOW - RT_FLOW_SESSION_CLOSE_LS
[junos@2636.1.1.1.2.34 logical-system-name="LSYS1" reason="response received"
source-address="3001::2" source-port="0" destination-address="5001::2"
destination-port="17420" service-name="icmpv6" nat-source-address="3001::2"
nat-source-port="0" nat-destination-address="5001::2" nat-destination-port="17420"
 src-nat-rule-name="None" dst-nat-rule-name="None" protocol-id="58"
policy-name="lsys1trust-to-lsys1trust" source-zone-name="lsys1-trust"
destination-zone-name="lsys1-trust" session-id-32="60000218"
packets-from-client="1" bytes-from-client="104" packets-from-server="1"
bytes-from-server="104" elapsed-time="3" application="UNKNOWN"
nested-application="UNKNOWN" username="N/A" roles="N/A"
packet-incoming-interface="ge-0/0/2.0" encrypted="No "]

 ...
```

show security log severity

Syntax show security log severity

Release Information Command introduced in Junos OS Release 15.1X49-D40.

Description Display severity information for the event.

Required Privilege Level view

Related Documentation

- show security log on page 162

Output Fields Table 35 on page 165 lists the output fields for the **show security log severity** command. Output fields are listed in the approximate order in which they appear.

Table 36: show security log severity Output Fields

Field Name	Field Description
alert	Alert severity
crit	Critical severity
debug	Debug severity
emerg	Emergency severity
err	Error severity
info	Information severity
notice	Notice severity
warning	Warning severity

show security log query

List of Syntax

Show Security Log Query on page 168
Show Security Log Stream on page 168

Show Security Log Query

```
show security log query {category all | utm | idp | alg | appqos | flow | fw-auth | gtp | ipsec |
   nat | pst-ds-lite | rtlog | screen | sctp | secintel} count < count>
[src-ip <src-ip>]
[dst-ip <dst-ip>]
[src-port <src-port>]
[dst-port <dst-port>]
[application <application>]
[user <user>]
[event-type <event-type>]
[service <service>]
[start-time <start-time>]
[stop-time <stop-time>]
```

Show Security Log Stream

```
show security log stream
file <filename>
```

Release Information

Command introduced in Junos OS Release 15.1X49-D70 for SRX1500, SRX4100, and SRX4200 Series devices and vSRX instances.

Description

- **show security log query**—View the security log from the database with query conditions.
- **show security log stream file**—View all the security log messages in the specified log file. Use the **/var/log/ hostlogs** directory to search the specified log file, and use the **show security log stream file** command to view logs in log files in the **/var/log/hostlogs** directory.

Options

- count—The log number to output.
- scr-ip—The source IP address of log messages.
- dst-ip—The destination IP address of log messages.
- src-port—The source port of log messages.
- dst-port—The destination port of log messages.
- application—The application of log messages.
- user—The user of log messages.
- event-type—The event type of log messages.
- service—The service of log messages.
- start-time—The earliest timestamp of log messages; the format for time is YYYY-MM-DDTHH:MM:SS.
- stop-time—The latest timestamp of log messages.

Required Privilege Level

view

Related Documentation

- *clear security log query*
- *clear security log stream file*

List of Sample Output

show security log query on page 169
show security log stream file <file-name> on page 169

Sample Output

show security log query

```
rootr@dut> show security log query category flow count 20 src-ip 211.0.0.2 start-time
2013-11-29T00:00:00 end-time 2013-11-29T23:59:00
<14>1 2013-11-29T16:01:26.820+08:00 plat02 RT_FLOW - RT_FLOW_SESSION_CLOSE
reason="CLI" source-address="211.0.0.2" source-port="20263"
destination-address="211.0.1.3" destination-port="4903" service-name="None"
nat-source-address="30.0.11.11" nat-source-port="27140"
nat-destination-address="211.0.1.3" nat-destination-port="4903"
src-nat-rule-name="src_rs2_rule1" dst-nat-rule-name="None" protocol-id="17"
policy-name="p1" source-zone-name="green" destination-zone-name="red"
session-id-32="30" packets-from-client="1" bytes-from-client="60"
packets-from-server="0" bytes-from-server="0" elapsed-time="92683"
application="UNKNOWN" nested-application="UNKNOWN" username="N/A" roles="N/A"
packet-incoming-interface="ge-0/0/1.0" encrypted="UNKNOWN"
```

show security log stream file <file-name>

```
root@dut> show security log stream file traffic.log
<14>1 2013-11-29T16:01:26.820+08:00 plat02 RT_FLOW - RT_FLOW_SESSION_CLOSE
reason="CLI" source-address="211.0.0.2" source-port="20263"
destination-address="211.0.1.3" destination-port="4903" service-name="None"
nat-source-address="30.0.11.11" nat-source-port="27140"
nat-destination-address="211.0.1.3" nat-destination-port="4903"
src-nat-rule-name="src_rs2_rule1" dst-nat-rule-name="None" protocol-id="17"
policy-name="p1" source-zone-name="green" destination-zone-name="red"
session-id-32="30" packets-from-client="1" bytes-from-client="60"
packets-from-server="0" bytes-from-server="0" elapsed-time="92683"
application="UNKNOWN" nested-application="UNKNOWN" username="N/A" roles="N/A"
packet-incoming-interface="ge-0/0/1.0" encrypted="UNKNOWN"] session closed CLI:
211.0.0.2/20263->211.0.1.3/4903 None 30.0.11.11/27140->211.0.1.3/4903 src_rs2_rule1
 None 17 p1 green red 30 1(60) 0(0) 92683 UNKNOWN UNKNOWN N/A(N/A) ge-0/0/1.0
UNKNOWN
```