Network Management and Monitoring Feature Guide for the QFX Series

Modified: 2018-02-12

Copyright © 2018, Juniper Networks, Inc.

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

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

Network Management and Monitoring Feature Guide for the QFX Series
Copyright © 2018 Juniper Networks, Inc. All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About the Documentation . . . xix
Documentation and Release Notes . . . xix
Supported Platforms . . . xix
Using the Examples in This Manual . . . xix
Merging a Full Example . . . xx
Merging a Snippet . . . xx
Documentation Conventions . . . xxi
Documentation Feedback . . . xxiii
Requesting Technical Support . . . xxiii
Self-Help Online Tools and Resources . . . xxiii
Opening a Case with JTAC . . . xxiv

Part 1 Network Management

Chapter 1 **Configuring Network Management . . . 3**

Understanding Device and Network Management Features . . . 3
Understanding Tracing and Logging Operations . . . 6
Configuring Console and Auxiliary Port Properties . . . 8
Configuring SSH Service for Remote Access to the Router or Switch . . . 9
Configuring the Root Login Through SSH . . . 10
Configuring the SSH Protocol Version . . . 10
Configuring the Client Alive Mechanism . . . 11
Configuring the SSH Fingerprint Hash Algorithm . . . 11
Configuring Telnet Service for Remote Access to a Switch . . . 11
Pinging Hosts . . . 12
Monitoring Traffic Through the Router or Switch . . . 13
Displaying Real-Time Statistics About All Interfaces on the Router or Switch . . . 13
Displaying Real-Time Statistics About an Interface on the Router or Switch . . . 14

Chapter 2 **Network Management Configuration Statements . . . 17**

connection-limit . . . 18
destination-override . . . 19
no-remote-trace . . . 19
protocol-version . . . 20
rate-limit . . . 21
ssh . . . 22
telnet . . . 23
tracing . . . 24

Chapter 3 Network Management Operational Commands 25
monitor traffic 26
ping 38

Part 2 Automation

Chapter 4 Configuring Automation 47
Overview of Junos Automation Enhancements 47
Features of the Junos Automation Enhancements 47
Overview of Python with Junos Automation Enhancements 48
Understanding Automation Scripts Support 51
How Commit Scripts Work 52
Commit Script Input 53
Commit Script Output 53
Commit Scripts and the Junos OS Commit Model 55
Standard Commit Model 56
Commit Model with Commit Scripts 56
Avoiding Potential Conflicts When Using Multiple Commit Scripts 58
Overview of Generating Persistent or Transient Configuration Changes Using Commit Scripts 59
Differences Between Persistent and Transient Changes 60
Interaction of Configuration Changes and Configuration Groups 63
Tag Elements and Templates for Generating Changes 63
Required Boilerplate for Commit Scripts 64
How Op Scripts Work 66
Required Boilerplate for Op Scripts 66
Installing Junos OS Software with Junos Automation Enhancements 68
Invoking the Python Interpreter 74
Controlling the Execution of Commit Scripts 74
Enabling Commit Scripts to Execute 75
Removing Commit Scripts from the Configuration 75
Deactivating Commit Scripts 76
Activating Inactive Commit Scripts 77
Displaying Commit Script Output 77

Chapter 5 Automation Configuration Statements 79
allow-transients 80
apply-macro 81
checksum 82
command 83
commit 84
description 85
direct-access 85
file (Commit Scripts) 86
file (Op Scripts) 87
no-allow-url (Op Scripts) 88
op 89
optional 90
refresh (Commit Scripts) 91

 Copyright © 2018, Juniper Networks, Inc.

refresh (Op Scripts) . . . 92
refresh-from (Commit Scripts) . . . 93
refresh-from (Op Scripts) . . . 94
scripts . . . 95
source (Commit Scripts) . . . 97
source (Op Scripts) . . . 98

Chapter 6 **Junos Space . . . 99**

Understanding Junos Space Support . . . 99

Part 3 Network Analytics

Chapter 7 **Configuring Network Analytics . . . 103**

Network Analytics Overview . . . 103
Analytics Feature Overview . . . 104
Network Analytics Enhancements Overview . . . 105
Summary of CLI Changes . . . 106
Understanding Network Analytics Configuration and Status . . . 111
Understanding Network Analytics Streaming Data . . . 112
Understanding Enhanced Network Analytics Streaming Data . . . 115
Google Protocol Buffer (GPB) . . . 115
JavaScript Object Notation (JSON) . . . 117
Comma-separated Values (CSV) . . . 118
Tab-separated Values (TSV) . . . 118
Queue Statistics Output for JSON, CSV, and TSV . . . 118
Traffic Statistics Output for JSON, CSV, and TSV . . . 119
Understanding Enhanced Analytics Local File Output . . . 120
Prototype File for the Google Protocol Buffer Stream Format . . . 122
Configuring Queue Monitoring . . . 123
Configuring Traffic Monitoring . . . 125
Configuring a Local File for Network Analytics Data . . . 126
Configuring a Remote Collector for Streaming Analytics Data . . . 127
Example: Configuring Network Analytics . . . 129

Chapter 8 **Network Analytics Configuration Statements . . . 137**

analytics . . . 138
depth-threshold . . . 142
interfaces (Analytics) . . . 144
latency-threshold . . . 146
queue-statistics . . . 148
streaming-servers . . . 150
traceoptions (Analytics) . . . 152
traffic-statistics . . . 153

Chapter 9 **Network Analytics Operational Commands . . . 155**

monitor start (Analytics) . . . 156
show analytics collector . . . 159
show analytics configuration . . . 161
show analytics queue-statistics . . . 165
show analytics status . . . 167

Copyright © 2018, Juniper Networks, Inc.

show analytics streaming-servers . . . 171
show analytics traffic-statistics . . . 173

Part 4 sFlow Technology

Chapter 10 **Configuring sFlow Technology . . . 179**

Understanding How to Use sFlow Technology for Network Monitoring on a Switch . . . 179
Sampling Mechanism and Architecture of sFlow Technology on Switches . . . 179
Adaptive Sampling . . . 181
sFlow Agent Address Assignment . . . 182
sFlow Limitations on Switches . . . 182
Configuring sFlow Technology . . . 184
Example: Monitoring Network Traffic Using sFlow Technology . . . 185

Chapter 11 **sFlow Technology Configuration Statements . . . 191**

agent-id . . . 191
collector (sFlow Technology) . . . 192
interfaces (sFlow) . . . 193
polling-interval . . . 194
sample-rate . . . 195
sflow . . . 196
source-ip . . . 197
traceoptions (sFlow Technology) . . . 198
udp-port . . . 199

Chapter 12 **sFlow Technology Operational Commands . . . 201**

clear sflow collector statistics . . . 202
show sflow . . . 203
show sflow collector . . . 205
show sflow interface . . . 206

Part 5 SNMP

Chapter 13 **Configuring SNMP . . . 211**

Understanding the Implementation of SNMP . . . 212
Utility MIB . . . 214
SNMPv3 Overview . . . 215
Minimum SNMPv3 Configuration on a Device Running Junos OS . . . 216
Understanding RMON . . . 217
RMON Overview . . . 217
Alarm Thresholds and Events . . . 218
RMON MIB Event, Alarm, Log, and History Control Tables . . . 219
Understanding Health Monitoring . . . 221
SNMP MIBs Support . . . 223
MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis . . . 223
MIBs Supported on QFabric Systems . . . 230

 Copyright © 2018, Juniper Networks, Inc.

SNMP Traps Support 236
SNMP Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis 236
SNMPv1 Traps 236
SNMPv2 Traps 240
SNMP Traps Supported on QFabric Systems 244
Juniper Networks Enterprise-Specific MIBs 248
MIB Objects for the QFX Series 251
QFX Series Standalone Switches 251
QFabric Systems 252
QFabric System QFX3100 Director Device 252
QFabric System QFX3008-I Interconnect Device 252
QFabric System QFX3600-I Interconnect Device 253
QFabric System Node Devices 253
Configuring SNMP 254
Configuring the SNMP Community String 257
Configuring SNMP Trap Groups 258
Adding a Group of Clients to an SNMP Community 259
Configuring the Interfaces on Which SNMP Requests Can Be Accepted 260
Configuring MIB Views 261
Configuring RMON Alarms and Events 262
Configuring SNMP 262
Configuring an Event 263
Configuring an Alarm 264
Configuring Health Monitoring 265
Creating SNMPv3 Users 266
Configuring Access Privileges for a Group 267
Assigning a Security Name to a Group 268
Configuring SNMPv3 Traps on a Device Running Junos OS 269
Configuring SNMP Informs 270
Monitoring RMON MIB Tables 271
Monitoring SNMP 272
Tracing SNMP Activity on a Device Running Junos OS 274
Configuring the Number and Size of SNMP Log Files 275
Configuring Access to the Log File 275
Configuring a Regular Expression for Lines to Be Logged 275
Configuring the Trace Operations 275
Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage 277
Example: Configuring SNMP 279

Chapter 14 **SNMP Configuration Statements 283**

access (SNMP) 286
address (SNMP) 287
address-mask 287
agent-address 288
alarm (SNMP RMON) 289
authentication-md5 290
authentication-none 291
authentication-password 292

authentication-sha . . . 293
authorization . . . 294
bucket-size . . . 295
categories . . . 296
client-list . . . 297
client-list-name . . . 297
clients . . . 298
commit-delay . . . 299
community (SNMP) . . . 300
community (RMON) . . . 301
community-name . . . 302
contact . . . 303
description . . . 303
description (RMON) . . . 304
destination-port (SNMP) . . . 305
engine-id . . . 306
event . . . 307
falling-event-index (RMON) . . . 308
falling-threshold (Health Monitor) . . . 309
falling-threshold (RMON) . . . 310
falling-threshold-interval . . . 311
filter-duplicates . . . 312
filter-interfaces . . . 312
group (Defining Access Privileges for an SNMPv3 Group) . . . 313
group (Configuring Group Name) . . . 314
health-monitor . . . 315
history . . . 316
interface (SNMP) . . . 317
interface (RMON) . . . 318
interval (Health Monitor) . . . 319
interval (RMON) . . . 320
local-engine . . . 321
location . . . 322
message-processing-model . . . 322
name . . . 323
nonvolatile . . . 323
notify . . . 324
notify-filter (Applying to the Management Target) . . . 325
notify-filter (Configuring the Profile Name) . . . 326
notify-view . . . 327
oid . . . 328
oid (SNMPv3) . . . 329
owner . . . 330
parameters . . . 331
port . . . 332
privacy-3des . . . 333
privacy-aes128 . . . 334
privacy-des . . . 335
privacy-none . . . 335

 Copyright © 2018, Juniper Networks, Inc.

privacy-password . . . 336
read-view . . . 337
remote-engine . . . 338
request-type . . . 339
retry-count . . . 340
rising-event-index . . . 341
rising-threshold (Health Monitor) . . . 342
rising-threshold (RMON) . . . 343
rmon . . . 344
sample-type . . . 345
security-level (Defining Access Privileges) . . . 346
security-level (Generating SNMP Notifications) . . . 347
security-model (Access Privileges) . . . 348
security-model (Group) . . . 349
security-model (SNMP Notifications) . . . 350
security-name (Community String) . . . 351
security-name (Security Group) . . . 352
security-name (SNMP Notifications) . . . 353
security-to-group . . . 354
snmp . . . 355
snmp-community . . . 359
source-address (SNMP) . . . 360
startup-alarm . . . 361
syslog-subtag . . . 362
tag (Configuring Notification Targets) . . . 363
tag-list . . . 364
target-address . . . 365
target-parameters . . . 366
targets . . . 367
timeout . . . 368
traceoptions (SNMP) . . . 369
trap-group . . . 371
trap-options . . . 372
type (RMON Notification) . . . 373
type . . . 374
user . . . 375
usm . . . 376
v3 . . . 378
vacm . . . 380
variable . . . 381
version . . . 382
view (Configuring a MIB View) . . . 383
view (Associating MIB View with a Community) . . . 384
write-view . . . 384

Chapter 15 SNMP Operational Commands . . . 385

clear snmp history . . . 386
clear snmp statistics . . . 387
request snmp spoof-trap . . . 389

request snmp utility-mib clear instance 395
request snmp utility-mib set instance 396
show snmp health-monitor 397
show snmp inform-statistics 402
show snmp mib 404
show snmp rmon 407
show snmp rmon history 411
show snmp statistics 412
show snmp v3 420

Part 6 System Logging

Chapter 16 **Configuring System Logging 425**

Overview of Junos OS System Log Messages 426
Overview of Single-Chassis System Logging Configuration 426
Junos OS Minimum System Logging Configuration 428
Junos OS System Log Configuration Statements 428
Adding a Text String to System Log Messages Directed to a Remote Destination 429
Directing System Log Messages to a Log File 430
Directing System Log Messages to a Remote Machine 431
Directing System Log Messages to a User Terminal 431
Directing System Log Messages to the Console 432
Disabling the System Logging of a Facility 432
Displaying a Log File from a Single-Chassis System 433
Including Priority Information in System Log Messages 434
Including the Year or Millisecond in Timestamps 435
Logging Messages in Structured-Data Format 436
Interpreting Messages Generated in Structured-Data Format 437
Interpreting Messages Generated in Standard Format 440
Specifying Log File Size, Number, and Archiving Properties 441
Specifying the Facility and Severity of Messages to Include in the Log 442
Junos OS System Logging Facilities and Message Severity Levels 444
Default Facilities for System Log Messages Directed to a Remote Destination 446
Alternate Facilities for System Log Messages Directed to a Remote Destination 446
Changing the Alternative Facility Name for System Log Messages Directed to a Remote Destination 447
Using Regular Expressions to Refine the Set of Logged Messages 449
Displaying a Log File from a Single-Chassis System 451
Monitoring System Log Messages 453
Examples: Configuring System Logging 454
Examples: Assigning an Alternative Facility 456
Example: Configuring System Log Messages 457

Chapter 17 **System Logging Configuration Statements 461**

archive (All System Log Files) 462
archive (Individual System Log File) 464
console (System Logging) 466

 Copyright © 2018, Juniper Networks, Inc.

explicit-priority 467
facility-override 468
file (System Logging) 469
files 470
host (System) 471
log-prefix (System) 473
match 474
size (System) 475
structured-data 476
syslog (System) 477
time-format 479
user (System Logging) 480

Chapter 18 System Logging Operational Commands 481

show log 482

Copyright © 2018, Juniper Networks, Inc.

List of Figures

Part 2 Automation

Chapter 4 **Configuring Automation 47**

Figure 1: Standard Commit Model 56
Figure 2: Commit Model with Commit Scripts Added 57
Figure 3: Configuration Evaluation by Multiple Commit Scripts 59

Part 4 sFlow Technology

Chapter 10 **Configuring sFlow Technology 179**

Figure 4: sFlow Technology Monitoring System 186

Part 5 SNMP

Chapter 13 **Configuring SNMP 211**

Figure 5: SNMP Communication Flow 213
Figure 6: Setting Thresholds 218
Figure 7: Inform Request and Response 271

Copyright © 2018, Juniper Networks, Inc.

Copyright © 2018, Juniper Networks, Inc.

List of Tables

About the Documentation xix

Table 1: Notice Icons xxi
Table 2: Text and Syntax Conventions xxii

Part 1 Network Management

Chapter 1 Configuring Network Management 3

Table 3: Device and Network Management Features on the QFX Series, OCX Series, and EX4600 3
Table 4: Output Control Keys for the monitor interface Command 15

Chapter 3 Network Management Operational Commands 25

Table 5: Match Conditions for the monitor traffic Command 28
Table 6: Logical Operators for the monitor traffic Command 30
Table 7: Arithmetic and Relational Operators for the monitor traffic Command 31

Part 2 Automation

Chapter 4 Configuring Automation 47

Table 8: Commit Scripts Actions and Output 54
Table 9: Differences Between Persistent and Transient Changes 61
Table 10: Commit Script Configuration and Operational Mode Commands 77

Part 3 Network Analytics

Chapter 7 Configuring Network Analytics 103

Table 11: Network Analytics CLI Changes 106
Table 12: Configuration and Status Output in Junos OS Release 13.2X51-D10 and 13.2X50-D15 111
Table 13: Streamed Queue Statistics Data Output Fields 113
Table 14: Streamed Traffic Statistics Data Output Fields 114
Table 15: GPB Stream Format Message Header Information 115
Table 16: Streamed Queue Statistics Data Output Fields 119
Table 17: Streamed Traffic Statistics Data Output Fields 119
Table 18: Output Fields for Queue Statistics in Local Analytics File 121
Table 19: Output Fields for Traffic Statistics in Local Analytics File 121

Chapter 9 Network Analytics Operational Commands 155

Table 20: monitor start Command Output Fields 156
Table 21: show analytics collector Command Output Fields 159

Table 22: show analytics configuration Command Output Fields (Junos OS Release 13.2X51-D15 and Later) 161
Table 23: show analytics configuration Command Output Fields (Junos OS Release 13.2X51-D10 and earlier) 162
Table 24: show analytics queue-statistics Command Output Fields 165
Table 25: show analytics status Command Output Fields 167
Table 26: show analytics streaming-servers Command Output Fields 171
Table 27: show analytics traffic-statistics Command Output Fields 173

Part 4 sFlow Technology

Chapter 12 **sFlow Technology Operational Commands 201**

Table 28: show sflow Output Fields 203
Table 29: show sflow collector Output Fields 205
Table 30: show sflow interface Output Fields 206

Part 5 SNMP

Chapter 13 **Configuring SNMP 211**

Table 31: RMON Event Table 219
Table 32: RMON Alarm Table 219
Table 33: jnxRmon Alarm Table 220
Table 34: RMON History Control Table 221
Table 35: Monitored Object Instances 222
Table 36: Standard MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis 223
Table 37: Juniper Networks Enterprise-Specific MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis 229
Table 38: Standard MIBs Supported on QFabric Systems 231
Table 39: Juniper Networks Enterprise-Specific MIBs Supported on QFabric Systems 234
Table 40: Standard SNMP Version 1 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis 236
Table 41: Enterprise-Specific SNMPv1 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis 239
Table 42: Standard SNMPv2 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis 241
Table 43: Enterprise-Specific SNMPv2 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis 243
Table 44: Standard SNMPv2 Traps Supported on QFabric Systems 245
Table 45: Enterprise-Specific SNMPv2 Traps Supported on QFabric Systems . . 246
Table 46: Juniper Networks Enterprise-Specific MIBs Supported on QFX3500 and QFX3600 Switches 248
Table 47: Juniper Networks Enterprise-Specific MIBs Supported on QFabric Systems 250
Table 48: SNMP Tracing Flags 276

Chapter 15 **SNMP Operational Commands 385**

Table 49: show snmp health-monitor Output Fields 397
Table 50: show snmp inform-statistics Output Fields 402

 Copyright © 2018, Juniper Networks, Inc.

Table 51: show snmp mib Output Fields 405
Table 52: show snmp rmon Output Fields 408
Table 53: show snmp statistics Output Fields 413
Table 54: show snmp statistics subagents Output Fields 416
Table 55: show snmp v3 Output Fields 421

Part 6 System Logging

Chapter 16 **Configuring System Logging 425**

Table 56: Minimum Configuration Statements for System Logging 428
Table 57: Fields in Structured-Data Messages 437
Table 58: Facility and Severity Codes in the priority-code Field 439
Table 59: Fields in Standard-Format Messages 440
Table 60: Junos OS System Logging Facilities 443
Table 61: System Log Message Severity Levels 444
Table 62: Junos OS System Logging Facilities 444
Table 63: System Log Message Severity Levels 445
Table 64: Default Facilities for Messages Directed to a Remote Destination . . . 446
Table 65: Facilities for the facility-override Statement 446
Table 66: Regular Expression Operators for the match Statement 450

Copyright © 2018, Juniper Networks, Inc.

Copyright © 2018, Juniper Networks, Inc.

About the Documentation

- Documentation and Release Notes on page xix
- Supported Platforms on page xix
- Using the Examples in This Manual on page xix
- Documentation Conventions on page xxi
- Documentation Feedback on page xxiii
- Requesting Technical Support on page xxiii

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:

- QFX 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; }
   ```


Copyright © 2018, Juniper Networks, Inc.

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 xxi defines notice icons used in this guide.

Table 1: Notice Icons

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

Table 2 on page xxii 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.	

GUI Conventions

Copyright © 2018, Juniper Networks, Inc.

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

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

Documentation Feedback

We encourage you to provide feedback, 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: https://prsearch.juniper.net/
- Find product documentation: http://www.juniper.net/documentation/
- 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://entitlementsearch.juniper.net/entitlementsearch/

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.

Copyright © 2018, Juniper Networks, Inc.

PART 1

Network Management

- Configuring Network Management on page 3
- Network Management Configuration Statements on page 17
- Network Management Operational Commands on page 25

Copyright © 2018, Juniper Networks, Inc.

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 1

Configuring Network Management

- Understanding Device and Network Management Features on page 3
- Understanding Tracing and Logging Operations on page 6
- Configuring Console and Auxiliary Port Properties on page 8
- Configuring SSH Service for Remote Access to the Router or Switch on page 9
- Configuring Telnet Service for Remote Access to a Switch on page 11
- Pinging Hosts on page 12
- Monitoring Traffic Through the Router or Switch on page 13

Understanding Device and Network Management Features

After you install a QFX Series product, OCX Series device, or EX4600 switch in your network, you need to manage the device. The products support features that you use to manage the device within the network, including the management of configuration, system performance, fault monitoring, and remote access.

Table 3 on page 3 lists the device and network management features on the QFX Series, OCX Series, and EX4600.

Table 3: Device and Network Management Features on the QFX Series, OCX Series, and EX4600

Feature	Typical Uses	Documentation
AI-Scripts and Advanced Insight Manager (AIM)—Automatically detect and monitor faults on the switch, and depending on the configuration on the AIM application, send notifications of potential problems, and submit problem reports to Juniper Support Systems.	Fault management	*Advanced Insight Scripts (AI-Scripts) Release Notes*
Alarms and LEDs on the switch—Show status of hardware components and indicate warning or error conditions.	Fault management	*Chassis Alarm Messages on a QFX3500 Device*
Firewall filters—Control the packets that are sent to and from the network, balance network traffic, and optimize performance.	Performance management	• *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide* • *Overview of Firewall Filters*

Copyright © 2018, Juniper Networks, Inc.

Table 3: Device and Network Management Features on the QFX Series, OCX Series, and EX4600 *(continued)*

Feature	Typical Uses	Documentation
In-band management—Enables connection to the switch using the same interfaces through which customer traffic flows. Communication between the switch and a remote console is typically enabled using SSH and Telnet services. SSH provides secure encrypted communications, whereas Telnet provides unencrypted, and therefore less secure, access to the switch.	Remote access management	• Configuring SSH Service for Remote Access to the Router or Switch on page 9 • *Configuring Telnet Service for Remote Access to a Router or Switch*
Juniper Networks Junos OS automation scripts—Configuration and operations automation tools provided by Junos OS. These tools include commit scripts, operation scripts, event scripts, and event policies. Commit scripts enforce custom configuration rules, whereas operation scripts, event policies, and event scripts automate network troubleshooting and management.	• Configuration management • Performance management • Fault management	*Automation Scripting Feature Guide*
Junos OS command-line interface (CLI)—CLI configuration statements that enable you to configure the switch based on your networking requirements, such as security, service, and performance.	• Configuration management • Performance management • User access management • Remote access management	*CLI User Guide*
Junos Space software—Multipurpose GUI-based network management system that includes a base platform, the Network Application Platform, and other optional applications such as Ethernet Design, Service Now, Service Insight, and Virtual Control. NOTE: Junos Space does not support the OCX Series.	• Configuration management • Performance management • Fault management	• Understanding Junos Space Support on page 99 • *Junos Space Network Application Platform User Guide*
Junos XML API—XML representation of Junos OS configuration statements and operational mode commands. Junos XML configuration tag elements are the content to which the Junos XML protocol operations apply. Junos XML operational tag elements are equivalent in function to operational mode commands in the CLI, which you can use to retrieve status information for a device. The Junos XML API also includes tag elements that are the counterpart to Junos CLI configuration statements.	• Configuration management • Performance management • Fault management	• *Junos XML API Configuration Developer Reference* • *Junos XML API Operational Developer Reference*

Copyright © 2018, Juniper Networks, Inc.

Table 3: Device and Network Management Features on the QFX Series, OCX Series, and EX4600 *(continued)*

Feature	Typical Uses	Documentation
NETCONF XML management protocol—XML-based management protocol that client applications use to request and change configuration information on routing, switching, and security platforms running Junos OS. The NETCONF XML management protocol defines basic operations that are equivalent to Junos OS CLI configuration mode commands. Client applications use the protocol operations to display, edit, and commit configuration statements (among other operations), just as administrators use CLI configuration mode commands such as **show**, **set**, and **commit** to perform those operations.	• Configuration management • Performance management • Fault management	*NETCONF XML Management Protocol Developer Guide*
Operational mode commands—May be used to do the following: • Monitor switch performance. For example, the **show chassis routing-engine** command shows the CPU utilization of the Routing Engine. High CPU utilization of the Routing Engine can affect performance of the switch. • View current activity and status of the device or network. For example, you can use the **ping** command to monitor and diagnose connectivity problems, and the **traceroute** command to locate points of failure on the network.	• Performance management • Fault management	CLI Explorer
Out-of-band management—Enables connection to the switch through a management interface. Out-of-band management is supported on two dedicated management Ethernet interfaces as well as on the console and auxiliary ports. The management Ethernet interfaces connect directly to the Routing Engine. No transit traffic is allowed through the interfaces, separating customer and management traffic and ensuring that congestion or failures in the transit network do not affect the management of the switch.	Remote access management	• *Connecting a Device to a Network for Out-of-Band Management* • *Connecting a QFX Series Device to a Management Console* • Configuring Console and Auxiliary Port Properties on page 8

Table 3: Device and Network Management Features on the QFX Series, OCX Series, and EX4600 *(continued)*

Feature	Typical Uses	Documentation
SNMP Configuration Management MIB—Provides notification for configuration changes in the form of SNMP traps. Each trap contains the time at which the configuration change was committed, the name of the user who made the change, and the method by which the change was made. A history of the last 32 configuration changes is kept in jnxCmChgEventTable.	Configuration management	SNMP MIB Explorer
SNMP MIBs and traps—Enable the monitoring of network devices from a central location. Use SNMP requests such as **get** and **walk** to monitor and view system activity. The QFX3500 switch supports SNMP Version 1 (v1), v2, and v3, and both standard and Juniper Networks enterprise-specific MIBs and traps.	Fault management	• SNMP MIB Explorer • Understanding the Implementation of SNMP on page 212
System log messages—Log details of system and user events, including errors. You can specify the severity and type of system log messages you wish to view or save, and configure the output to be sent to local or remote hosts.	• Fault management • User access management	• System Log Explorer • Overview of Junos OS System Log Messages on page 426 • Overview of Single-Chassis System Logging Configuration on page 426

Understanding Tracing and Logging Operations

Tracing and logging operations enable you to track events that occur in the switch—both normal operations and error conditions—and to track the packets that are generated by or passed through the switch. The results of tracing and logging operations are placed in files in the **/var/log** directory on the switch.

The Junos OS supports remote tracing for the following processes:

- **chassisd**—Chassis-control process
- **eventd**—Event-processing process
- **cosd**—Class-of-service process

You configure remote tracing by using the **tracing** statement at the **[edit system]** hierarchy level.

NOTE: **The tracing statement is not supported on the QFX3000 QFabric system.**

Copyright © 2018, Juniper Networks, Inc.

If you enabled remote tracing but wish to disable it for specific processes on the switch, use the **no-remote-trace** statement at the **[edit *process-name* traceoptions]** hierarchy level. This feature does not alter local tracing functionality in any way, and logging files are stored on the switch.

Logging operations use a system logging mechanism similar to the UNIX **syslogd** utility to record systemwide, high-level operations, such as interfaces going up or down and users logging in to or out of the switch. You configure these operations by using the **syslog** statement at the **[edit system]** hierarchy level and by using the **options** statement at the **[edit ethernet-switching-options]** hierarchy level.

Tracing operations record more detailed information about the operations of the switch, including packet forwarding and routing information. To configure tracing operations, use the **traceoptions** statement.

NOTE: The **traceoptions** statement is not supported on the QFX3000 QFabric system.

You can define tracing operations in different portions of the switch configuration:

- SNMP agent activity tracing operations—Define tracing of the activities of SNMP agents on the switch. You configure SNMP agent activity tracing operations at the **[edit snmp]** hierarchy level.
- Global switching tracing operations—Define tracing for all switching operations. You configure global switching tracing operations at the **[edit ethernet-switching-options]** hierarchy level of the configuration.
- Protocol-specific tracing operations—Define tracing for a specific routing protocol. You configure protocol-specific tracing operations in the **[edit protocols]** hierarchy when configuring the individual routing protocol. Protocol-specific tracing operations override any equivalent operations that you specify in the global **traceoptions** statement. If there are no equivalent operations, they supplement the global tracing options. If you do not specify any protocol-specific tracing, the routing protocol inherits all the global tracing operations.
- Tracing operations within individual routing protocol entities—Some protocols allow you to define more granular tracing operations. For example, in Border Gateway Protocol (BGP), you can configure peer-specific tracing operations. These operations override any equivalent BGP-wide operations or, if there are no equivalents, supplement them. If you do not specify any peer-specific tracing operations, the peers inherit, first, all the BGP-wide tracing operations and, second, the global tracing operations.
- Interface tracing operations—Define tracing for individual interfaces and for the interface process itself. You define interface tracing operations at the **[edit interfaces]** hierarchy level of the configuration.
- Remote tracing—To enable system-wide remote tracing, configure the **destination-override syslog host** statement at the **[edit system tracing]** hierarchy level. This specifies the remote host running the system log process (syslogd), which collects

the traces. Traces are written to files on the remote host in accordance with the syslogd configuration in **/etc/syslog.conf**. By default, remote tracing is not configured.

To override the system-wide remote tracing configuration for a particular process, include the **no-remote-trace** statement at the **[edit *process-name* traceoptions]** hierarchy. When **no-remote-trace** is enabled, the process does local tracing.

To collect traces, use the **local0** facility as the selector in the **/etc/syslog.conf** file on the remote host. To separate traces from various processes into different files, include the process name or trace-file name (if it is specified at the [edit ***process-name*** **traceoptions file**] hierarchy level) in the Program field in the **/etc/syslog.conf** file. If your system log server supports parsing hostname and program name, then you can separate traces from the various processes.

NOTE: During a commit check, warnings about the **traceoptions** configuration (for example, mismatch in trace file sizes or number of trace files) are not displayed on the console. However, these warnings are logged in the system log messages when the new configuration is committed.

Related Documentation

- Overview of Junos OS System Log Messages on page 426

Configuring Console and Auxiliary Port Properties

The console port and auxiliary port on a switch provide out-of-band remote access to the switch. You can configure the console and auxiliary ports so that an external data terminal may be connected to the switch. The console port is enabled by default. The console port speed is 9600 baud, except on OCX Series devices, on which it is 115200 baud. The auxiliary port is disabled by default.

By default, terminal connections to the console and auxiliary ports are secure. When you configure the console and auxiliary ports as insecure, root logins are not allowed to establish terminal connections, and superusers and anyone with a user identifier (UID) of 0 are not allowed to establish terminal connections in multiuser mode.

To configure the console and auxiliary port properties on the switch:

1. To specify that the console port session should terminate if the connection to the data carrier is lost:

   [edit system ports]
   user@switch# **set console log-out-on-disconnect**

2. To specify the auxiliary port terminal type:

   [edit system ports]
   user@switch# **set auxiliary type (ansi | small-xterm | vt100 | xterm)**

   For example, to specify the auxiliary port terminal type of **xterm** with a display of 80 columns by 65 rows:

Copyright © 2018, Juniper Networks, Inc.

```
[edit system ports]
user@switch# set auxiliary type xterm
```

3. To check the configuration:

```
[edit system ports]
user@switch# show
console log-out-on-disconnect;
auxiliary type xterm;
```

Related Documentation

- *auxiliary*
- *console (Physical Port)*
- *ports*

Configuring SSH Service for Remote Access to the Router or Switch

To configure the router or switch to accept SSH as an access service, include the **ssh** statement at the **[edit system services]** hierarchy level:

```
[edit system services]
ssh {
  authentication-order [method 1 method2...];
  ciphers [ cipher-1 cipher-2 cipher-3 ...];
  client-alive-count-max seconds;
  client-alive-interval seconds;
  connection-limit limit;
  fingerprint-hash (md5 | sha2-256);
  hostkey-algorithm (algorithm | no-algorithm);
  key-exchange [algorithm1 algorithm2...];
  macs [algorithm1 algorithm2...];
  max-sessions-per-connection <number>;
  no-passwords;
  no-public-keys;
  no-tcp-forwarding;
  protocol-version [v2];
  rate-limit limit;
  root-login (allow | deny | deny-password);
  }
}
```

By default, the router or switch supports a limited number of simultaneous SSH sessions and connection attempts per minute. Use the following statements to change the defaults:

- **connection-limit** ***limit***—Maximum number of simultaneous connections per protocol (IPv4 and IPv6). The range is a value from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of SSH sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 SSH sessions and 10 IPv4 SSH sessions.
- **max-sessions-per-connection** ***number***—Include this statement to specify the maximum number of SSH sessions allowed per single SSH connection. This allows you to limit

the number of cloned sessions tunneled within a single SSH connection. The default value is 10.

- **rate-limit** ***limit***—Maximum number of connection attempts accepted per minute (a value from 1 through 250). The default is 150. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 SSH session connection attempts per minute and 10 IPv4 SSH session connection attempts per minute.

By default, a user can create an SSH tunnel over a CLI session to a router running Junos OS via SSH. This type of tunnel could be used to forward TCP traffic, bypassing any firewall filters or access control lists allowing access to resources beyond the router. Use the **no-tcp-forwarding** option to prevent a user from creating an SSH tunnel to a router via SSH.

For information about other configuration settings, see the following topics:

- Configuring the Root Login Through SSH on page 10
- Configuring the SSH Protocol Version on page 10
- Configuring the Client Alive Mechanism on page 11
- Configuring the SSH Fingerprint Hash Algorithm on page 11

Configuring the Root Login Through SSH

By default, users are allowed to log in to the router or switch as **root** through SSH when the authentication method does not require a password. To control user access through SSH, include the **root-login** statement at the **[edit systems services ssh]** hierarchy level:

```
[edit system services ssh]
root-login (allow | deny | deny-password);
```

allow—Allows users to log in to the router or switch as root through SSH.

deny—Disables users from logging in to the router or switch as root through SSH.

deny-password—Allows users to log in to the router or switch as root through SSH when the authentication method (for example, RSA) does not require a password.

The default is **deny-password**.

Configuring the SSH Protocol Version

By default, only version 2 of the SSH protocol is enabled.

To configure the router or switch to use version 2 of the SSH protocol, include the **protocol-version** statement and specify **v2** at the **[edit system services ssh]** hierarchy level:

```
[edit system services ssh]
protocol-version [ v2 ];
```

Systems in FIPS mode always use SSH protocol version **v2**.

Copyright © 2018, Juniper Networks, Inc.

Configuring the Client Alive Mechanism

The client alive mechanism is valuable when the client or server depends on knowing when a connection has become inactive. It differs from the standard keepalive mechanism because the client alive messages are sent through the encrypted channel. The client alive mechanism is not enabled at default. To enable it, configure the **client-alive-count-max** and **client-alive-interval** statements. This option applies to SSH protocol version 2 only.

In the following example, unresponsive SSH clients will be disconnected after approximately 100 seconds (20 x 5).

```
[edit system services ssh]
client-alive-count-max 5;
client-alive-interval 20;
```

See Also

- ssh on page 22

Configuring the SSH Fingerprint Hash Algorithm

To configure the hash algorithm used by the SSH server when it displays key fingerprints, include the **fingerprint-hash** statement and specify **md5** or **sha2-256** at the **[edit system services ssh]** hierarchy level:

```
[edit system services ssh]
fingerprint-hash (md5 | sha2-256);
```

The **md5** hash algorithm is unavailable on systems in FIPS mode.

See Also

- ssh on page 22

Configuring Telnet Service for Remote Access to a Switch

Telnet provides unencrypted access to network devices. Configuring Telnet service for a switch enables in-band remote access to the switch.

By default, the switch supports a limited number of simultaneous Telnet sessions and connection attempts per minute. Optionally, you can change the default Telnet settings by configuring the connection limit and rate limit at the **[edit system services telnet]** hierarchy level.

The connection limit is the maximum number of simultaneous connections per protocol (IPv4). The range is from **1** through **250**. The default is **75**.

The rate limit is the maximum number of connection attempts accepted per minute per protocol. The range is from **1** through **250**. The default is **150**.

To configure Telnet service:

1. To specify the connection limit:

```
[edit system services]
user@switch# set telnet connection-limit connection-limit
```

2. To specify the rate limit:

```
[edit system services]
user@switch# set telnet rate-limit rate-limit
```

3. Check that the Telnet connection limit and rate limit show the values you specified:

```
[edit system services]
user@switch# show
  telnet {
    connection-limit 50;
    rate-limit 100;
  }
```

Related Documentation

- *Understanding Telnet on the QFabric System*
- *Example: Limiting the Number of Login Attempts for SSH and Telnet Sessions to Prevent Unauthorized Access*

Pinging Hosts

Purpose

Use the CLI **ping** command to verify that a host can be reached over the network. This command is useful for diagnosing host and network connectivity problems. The switch sends a series of Internet Control Message Protocol (ICMP) echo (ping) requests to a specified host and receives ICMP echo responses.

Action

To use the **ping** command to send four requests (ping count) to host3:

ping *host* **count** *number*

Sample Output

ping host3 count 4

```
user@switch> ping host3 count 4
PING host3.site.net (192.0.2.111): 56 data bytes
64 bytes from 192.0.2.111: icmp_seq=0 ttl=122 time=0.661 ms
64 bytes from 192.0.2.111: icmp_seq=1 ttl=122 time=0.619 ms
64 bytes from 192.0.2.111: icmp_seq=2 ttl=122 time=0.621 ms
64 bytes from 192.0.2.111: icmp_seq=3 ttl=122 time=0.634 ms

--- host3.site.net ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.619/0.634/0.661/0.017 ms
```

Meaning

- The **ping** results show the following information:
  - Size of the ping response packet (in bytes).
  - IP address of the host from which the response was sent.

Copyright © 2018, Juniper Networks, Inc.

- Sequence number of the ping response packet. You can use this value to match the ping response to the corresponding ping request.
- Time-to-live (ttl) hop-count value of the ping response packet.
- Total time between the sending of the ping request packet and the receiving of the ping response packet, in milliseconds. This value is also called round-trip time.
- Number of ping requests (probes) sent to the host.
- Number of ping responses received from the host.
- Packet loss percentage.
- Round-trip time statistics: minimum, average, maximum, and standard deviation of the round-trip time.

Related Documentation

- *Troubleshooting Overview*
- *Understanding Troubleshooting Resources*

Monitoring Traffic Through the Router or Switch

To help with the diagnosis of a problem, display real-time statistics about the traffic passing through physical interfaces on the router or switch.

To display real-time statistics about physical interfaces, perform these tasks:

1. Displaying Real-Time Statistics About All Interfaces on the Router or Switch on page 13
2. Displaying Real-Time Statistics About an Interface on the Router or Switch on page 14

Displaying Real-Time Statistics About All Interfaces on the Router or Switch

Purpose Display real-time statistics about traffic passing through all interfaces on the router or switch.

Action To display real-time statistics about traffic passing through all interfaces on the router or switch:

user@host> **monitor interface traffic**

Sample Output

```
user@host> monitor interface traffic
host name                  Seconds: 15                  Time: 12:31:09
Interface     Link  Input packets        (pps)     Output packets        (pps)
 so-1/0/0     Down              0          (0)                  0          (0)
 so-1/1/0     Down              0          (0)                  0          (0)
 so-1/1/1     Down              0          (0)                  0          (0)
 so-1/1/2     Down              0          (0)                  0          (0)
 so-1/1/3     Down              0          (0)                  0          (0)
 t3-1/2/0     Down              0          (0)                  0          (0)
 t3-1/2/1     Down              0          (0)                  0          (0)
```

```
 t3-1/2/2    Down              0          (0)                  0          (0)
 t3-1/2/3    Down              0          (0)                  0          (0)
 so-2/0/0      Up         211035           (1)              36778           (0)
 so-2/0/1      Up         192753          (1)              36782          (0)
 so-2/0/2      Up         211020          (1)              36779          (0)
 so-2/0/3      Up         211029          (1)              36776          (0)
 so-2/1/0      Up         189378          (1)              36349          (0)
 so-2/1/1    Down              0          (0)              18747          (0)
 so-2/1/2    Down              0          (0)              16078          (0)
 so-2/1/3      Up              0          (0)              80338          (0)
 at-2/3/0      Up              0          (0)                  0          (0)
 at-2/3/1    Down              0          (0)                  0          (0)
Bytes=b, Clear=c, Delta=d, Packets=p, Quit=q or ESC, Rate=r, Up=^U, Down=^D
```

Meaning The sample output displays traffic data for active interfaces and the amount that each field has changed since the command started or since the counters were cleared by using the **C** key. In this example, the **monitor interface** command has been running for 15 seconds since the command was issued or since the counters last returned to zero.

Displaying Real-Time Statistics About an Interface on the Router or Switch

Purpose Display real-time statistics about traffic passing through an interface on the router or switch.

Action To display traffic passing through an interface on the router or switch, use the following Junos OS CLI operational mode command:

user@host> **monitor interface** ***interface-name***

Sample Output

```
user@host> monitor interface so-0/0/1
Next='n', Quit='q' or ESC, Freeze='f', Thaw='t', Clear='c', Interface='i'
R1
Interface: so-0/0/1, Enabled, Link is Up
Encapsulation: PPP, Keepalives, Speed: OC3 Traffic statistics:
  Input bytes:                    5856541 (88 bps)
  Output bytes:                   6271468 (96 bps)
  Input packets:                   157629 (0 pps)
  Output packets:                  157024 (0 pps)
Encapsulation statistics:
  Input keepalives:                 42353
  Output keepalives:                42320
  LCP state: Opened
Error statistics:
  Input errors:                         0
  Input drops:                          0
  Input framing errors:                 0
  Input runts:                          0
  Input giants:                         0
  Policed discards:                     0
  L3 incompletes:                       0
  L2 channel errors:                    0
  L2 mismatch timeouts:                 0
  Carrier transitions:                  1
```

 Copyright © 2018, Juniper Networks, Inc.

```
  Output errors:                        0
  Output drops:                         0
  Aged packets:                         0
Active alarms : None
Active defects: None
SONET error counts/seconds:
  LOS count                             1
  LOF count                             1
  SEF count                             1
  ES-S                                 77
  SES-S                                77
SONET statistics:
  BIP-B1                                0
  BIP-B2                                0
  REI-L                                 0
  BIP-B3                                0
  REI-P                                 0
Received SONET overhead:  F1        : 0x00  J0        : 0xZ
```

Meaning The sample output shows the input and output packets for a particular SONET interface (**so-0/0/1**). The information can include common interface failures, such as SONET/SDH and T3 alarms, loopbacks detected, and increases in framing errors. For more information, see *Checklist for Tracking Error Conditions*.

To control the output of the command while it is running, use the keys shown in Table 4 on page 15.

Table 4: Output Control Keys for the monitor interface Command

Action	Key
Display information about the next interface. The **monitor interface** command scrolls through the physical or logical interfaces in the same order that they are displayed by the **show interfaces terse** command.	N
Display information about a different interface. The command prompts you for the name of a specific interface.	I
Freeze the display, halting the display of updated statistics.	F
Thaw the display, resuming the display of updated statistics.	T
Clear (zero) the current delta counters since **monitor interface** was started. It does not clear the accumulative counter.	C
Stop the **monitor interface** command.	Q

See the CLI Explorer for details on using match conditions with the **monitor traffic** command.

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 2

Network Management Configuration Statements

- connection-limit on page 18
- destination-override on page 19
- no-remote-trace on page 19
- protocol-version on page 20
- rate-limit on page 21
- ssh on page 22
- telnet on page 23
- tracing on page 24

Copyright © 2018, Juniper Networks, Inc.

connection-limit

Syntax connection-limit *limit*;

Hierarchy Level
[edit system services finger],
[edit system services ftp],
[edit system services netconf ssh],
[edit system services ssh],
[edit system services telnet],
[edit system services xnm-clear-text],
[edit system services xnm-ssl]

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 OCX Series switches.

Description Configure the maximum number of connections sessions for each type of system services (finger, ftp, ssh, telnet, xnm-clear-text, or xnm-ssl) per protocol (either IPv6 or IPv4).

Options ***limit***—(Optional) Maximum number of established connections per protocol (either IPv6 or IPv4).

Range: 1 through 250

Default: 75

NOTE: **The actual number of maximum connections depends on the availability of system resources, and might be fewer than the configured connection-limit value if the system resources are limited.**

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

Related Documentation

- *Configuring clear-text or SSL Service for Junos XML Protocol Client Applications*
- *Configuring DTCP-over-SSH Service for the Flow-Tap Application*
- *Configuring Finger Service for Remote Access to the Router*
- *Configuring FTP Service for Remote Access to the Router or Switch*
- Configuring SSH Service for Remote Access to the Router or Switch on page 9
- *Configuring Telnet Service for Remote Access to a Router or Switch*

Copyright © 2018, Juniper Networks, Inc.

destination-override

Syntax

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

Hierarchy Level [edit system tracing]

Release Information 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 Override the system-wide configuration of the switch at the **[edit system tracing]** hierarchy level. This statement has no effect if system tracing is not configured.

Options **syslog**—System process log files to send to the remote tracing host.

- **syslog**—System process log files to send to the remote tracing host.
- **host *ip-address***—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

- Understanding Tracing and Logging Operations on page 6
- tracing on page 24

no-remote-trace

Syntax no-remote-trace

Hierarchy Level [edit system]

Release Information 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 switch to disable remote tracing after remote tracing has been enabled.

Default Remote tracing is disabled.

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

Related Documentation

- tracing on page 24

protocol-version

Syntax protocol-version [v2];

Hierarchy Level [edit system services ssh]

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 OCX Series switches.

Description Specify the Secure Shell (SSH) protocol version.

Default **v2**—SSH protocol version 2 is the default, introduced in Junos OS Release 11.4.

Options SSH protocol version **v2**.

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

Related Documentation

- Configuring the SSH Protocol Version on page 10

 Copyright © 2018, Juniper Networks, Inc.

rate-limit

Syntax

rate-limit *limit*;

Hierarchy Level

[edit system services finger],
[edit system services ftp],
[edit system services netconf ssh],
[edit system services ssh],
[edit system services telnet],
[edit system services tftp-server],
[edit system services xnm-clear-text],
[edit system services xnm-ssl]

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

Description

Configure the maximum number of connections attempts per minute, per protocol (either IPv6 or IPv4) on an access service. For example, a rate limit of 10 allows 10 IPv6 telnet session connection attempts per minute and 10 IPv4 telnet session connection attempts per minute.

Default

150 connections

Options

rate-limit *limit*—(Optional) Maximum number of connection attempts allowed per minute, per IP protocol (either IPv4 or IPv6).

Range: 1 through 250

Default: 150

Required Privilege Level

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

Related Documentation

- *Configuring clear-text or SSL Service for Junos XML Protocol Client Applications*

ssh

Syntax

```
ssh {
   authentication-order [method 1 method2...];
   ciphers [ cipher-1 cipher-2 cipher-3 ...];
   client-alive-count-max seconds;
   client-alive-interval seconds;
   connection-limit limit;
   fingerprint-hash (md5 | sha2-256);
   hostkey-algorithm (algorithm | no-algorithm);
   key-exchange [algorithm1 algorithm2...];
   macs [algorithm1 algorithm2...];
   max-sessions-per-connection <number>;
   no-passwords;
   no-public-keys;
   no-tcp-forwarding;
   protocol-version [v2];
   rate-limit limit;
   root-login (allow | deny | deny-password);
   }
tcp-forwarding (JDM)
```

Hierarchy Level

[edit system services]

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.
client-alive-interval and **client-alive-max-count** statements introduced in Junos OS Release 12.2.
no-passwords statement introduced in Junos OS Release 13.3.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
no-public-keys statement introduced in Junos OS release 15.1.
tcp-forwarding statement introduced in Junos OS Release 15.1X53-D50 for the NFX250 Network Services Platform.
fingerprint-hash statement introduced in Junos OS Release 16.1.

Description

Allow SSH requests from remote systems to access the local router or switch.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- Configuring SSH Service for Remote Access to the Router or Switch on page 9

Copyright © 2018, Juniper Networks, Inc.

telnet

Syntax

```
telnet {
   authentication-order [authentication-methods];
   connection-limit limit;
   rate-limit limit;
}
```

Hierarchy Level

[edit system services]

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

Provide Telnet connections from remote systems to the local router or switch.

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

- *Configuring Telnet Service for Remote Access to a Router or Switch*

tracing

Syntax

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

Hierarchy Level

[edit system]

Release Information

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 switch to enable remote tracing to a specified host IP address.

NOTE: **The tracing statement is not supported on the QFX3000 QFabric system.**

The following processes are supported:

- **chassisd**—Chassis-control process
- **eventd**—Event-processing process
- **cosd**—Class-of-service process

If you enabled remote tracing but wish to disable it for specific processes on the switch, use the **no-remote-trace** statement at the **[edit system *process-name* traceoptions]** hierarchy level.

Default

Remote tracing is disabled by default.

Options

destination-override syslog host *ip-address*—Overrides the global configuration for system tracing and has no effect if the **tracing** statement 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

- Understanding Tracing and Logging Operations on page 6
- destination-override on page 19

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 3

Network Management Operational Commands

- monitor traffic
- ping

monitor traffic

Syntax

monitor traffic
<brief | detail | extensive>
<absolute-sequence>
<count *count*>
<interface *interface-name*>
<layer2-headers>
<matching *matching*>
<no-domain-names>
<no-promiscuous>
<no-resolve>
<no-timestamp>
<print-ascii>
<print-hex>
<resolve-timeout>
<size *size*>

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 the OCX Series.

Description

Display packet headers or packets received and sent from the Routing Engine.

NOTE:

- Using the **monitor-traffic** command can degrade router or switch performance.
- Delays from DNS resolution can be eliminated by using the **no-resolve** option.

NOTE: This command is not supported on the QFabric system.

Options

none—(Optional) Display packet headers transmitted through **fxp0**. On a TX Matrix Plus router, display packet headers transmitted through **em0**.

brief | detail | extensive—(Optional) Display the specified level of output.

absolute-sequence—(Optional) Display absolute TCP sequence numbers.

count *count*—(Optional) Specify the number of packet headers to display (0 through 1,000,000). The monitor traffic command quits automatically after displaying the number of packets specified.

Copyright © 2018, Juniper Networks, Inc.

interface *interface-name*—(Optional) Specify the interface on which the **monitor traffic** command displays packet data. If no interface is specified, the **monitor traffic** command displays packet data arriving on the lowest-numbered interface.

layer2-headers—(Optional) Display the link-level header on each line.

matching *matching*—(Optional) Display packet headers that match a regular expression. Use matching expressions to define the level of detail with which the **monitor traffic** command filters and displays packet data.

no-domain-names—(Optional) Suppress the display of the domain portion of hostnames. With the **no-domain-names** option enabled, the **monitor traffic** command displays only **team** for the hostname **team.company.net**.

no-promiscuous—(Optional) Do not put the interface into promiscuous mode.

no-resolve—(Optional) Suppress reverse lookup of the IP addresses.

no-timestamp—(Optional) Suppress timestamps on displayed packets.

print-ascii—(Optional) Display each packet in ASCII format.

print-hex—(Optional) Display each packet, except the link-level header, in hexadecimal format.

resolve-timeout *timeout*—(Optional) Amount of time the router or switch waits for each reverse lookup before timing out. You can set the timeout for 1 through 4,294,967,295 seconds. The default is 4 seconds. To display each packet, use the **print-ascii**, **print-hex**, or **extensive** option.

size *size*—(Optional) Read but do not display up to the specified number of bytes for each packet. When set to **brief** output, the default packet size is 96 bytes and is adequate for capturing IP, ICMP, UDP, and TCP packet data. When set to **detail** and **extensive** output, the default packet size is 1514. The **monitor traffic** command truncates displayed packets if the matched data exceeds the configured size.

Additional Information

In the **monitor traffic** command, you can specify an expression to match by using the **matching** option and including the expression in quotation marks:

```
monitor traffic matching "expression"
```

Replace ***expression*** with one or more of the match conditions listed in Table 5 on page 28.

Table 5: Match Conditions for the monitor traffic Command

Match Type	Condition	Description
Entity	**host** [*address* | *hostname*]	Matches packets that contain the specified address or hostname. The protocol match conditions **arp**, **ip**, or **rarp**, or any of the directional match conditions can be prepended to the **host** match condition.
	net *address*	Matches packets with source or destination addresses containing the specified network address.
	net *address* **mask** *mask*	Matches packets containing the specified network address and subnet mask.
	port (*port-number* | *port-name*)	Matches packets containing the specified source or destination TCP or UDP port number or port name. In place of the numeric port address, you can specify a text synonym, such as **bgp** (179), **dhcp** (67), or **domain** (53) (the port numbers are also listed).
Directional	**dst**	Matches packets going to the specified destination. This match condition can be prepended to any of the entity type match conditions.
	src	Matches packets from a specified source. This match condition can be prepended to any of the entity type match conditions.
	src and **dst**	Matches packets that contain the specified source and destination addresses. This match condition can be prepended to any of the entity type match conditions.
	src or **dst**	Matches packets containing either of the specified addresses. This match condition can be prepended to any of the entity type match conditions.
Packet Length	**less** *value*	Matches packets shorter than or equal to the specified value, in bytes.
	greater *value*	Matches packets longer than or equal to the specified value, in bytes.

Copyright © 2018, Juniper Networks, Inc.

Table 5: Match Conditions for the monitor traffic Command *(continued)*

Match Type	Condition	Description
Protocol	**amt**	Matches all AMT packets. Use the extensive level of output to decode the inner IGMP packets in addition to the AMT outer packet.
	arp	Matches all ARP packets.
	ether	Matches all Ethernet packets.
	ether (broadcast | multicast)	Matches broadcast or multicast Ethernet frames. This match condition can be prepended with**src** and **dst**.
	ether *protocol* **(***address* **| (arp | ip | rarp))**	Matches packets with the specified Ethernet address or Ethernet packets of the specified protocol type. The **ether protocol** arguments **arp**, **ip**, and **rarp** are also independent match conditions, so they must be preceded by a backslash (\) when used in the **ether protocol** match condition.
	icmp	Matches all ICMP packets.
	ip	Matches all IP packets.
	ip (broadcast | multicast)	Matches broadcast or multicast IP packets.
	ip protocol (*address* **| (icmp | igrp | tcp | udp))**	Matches packets with the specified address or protocol type. The **ip protocol** arguments **icmp**, **tcp**, and **udp** are also independent match conditions, so they must be preceded by a backslash (\) when used in the **ip protocol** match condition.
	isis	Matches all IS-IS routing messages.
	proto *ip-protocol-number*	Matches packets whose headers contain the specified IP protocol number.
	rarp	Matches all RARP packets.
	tcp	Matches all TCP datagrams.
	udp	Matches all UDP datagrams.

To combine expressions, use the logical operators listed in Table 6 on page 30.

Table 6: Logical Operators for the monitor traffic Command

Logical Operator (Highest to Lowest Precedence)	Description
!	Logical NOT. If the first condition does not match, the next condition is evaluated.
&&	Logical AND. If the first condition matches, the next condition is evaluated. If the first condition does not match, the next condition is skipped.
||	Logical OR. If the first condition matches, the next condition is skipped. If the first condition does not match, the next condition is evaluated.
( )	Group operators to override default precedence order. Parentheses are special characters, each of which must be preceded by a backslash (\).

You can use relational operators to compare arithmetic expressions composed of integer constants, binary operators, a length operator, and special packet data accessors. The arithmetic expression matching condition uses the following syntax:

monitor traffic matching "ether[0] & 1 != 0"*"arithmetic_expression relational_operator arithmetic_expression"*

The packet data accessor uses the following syntax:

protocol [byte-offset <*size*>]

The optional *size* field represents the number of bytes examined in the packet header. The available values are **1, 2,** or **4** bytes. The following sample command captures all multicast traffic:

user@host> **monitor traffic matching "ether[0] & 1 != 0"**

To specify match conditions that have a numeric value, use the arithmetic and relational operators listed in Table 7 on page 31.

 Copyright © 2018, Juniper Networks, Inc.

NOTE: Because the Packet Forwarding Engine removes Layer 2 header information before sending packets to the Routing Engine:

- The **monitor traffic** command cannot apply match conditions to inbound traffic.
- The **monitor traffic interface** command also cannot apply match conditions for Layer 3 and Layer 4 packet data, resulting in the **match** pipe option (**| match**) for this command for Layer 3 and Layer 4 packets not working either. Therefore, ensure that you specify match conditions as described in this command summary. For more information about match conditions, see Table 5 on page 28.
- The 802.1Q VLAN tag information included in the Layer 2 header is removed from all inbound traffic packets. Because the **monitor traffic interface ae[*x*]** command for aggregated Ethernet interfaces (such as **ae0**) only shows inbound traffic data, the command does not show VLAN tag information in the output.

Table 7: Arithmetic and Relational Operators for the monitor traffic Command

Arithmetic or Relational Operator	Description
Arithmetic Operator	
+	Addition operator.
-	Subtraction operator.
/	Division operator.
&	Bitwise AND.
*	Bitwise exclusive OR.
|	Bitwise inclusive OR.
Relational Operator (Highest to Lowest Precedence)	
<=	If the first expression is less than or equal to the second, the packet matches.
>=	If the first expression is greater than or equal to the second, the packet matches.
<	If the first expression is less than the second, the packet matches.
>	If the first expression is greater than the second, the packet matches.

Copyright © 2018, Juniper Networks, Inc.

Table 7: Arithmetic and Relational Operators for the monitor traffic Command *(continued)*

Arithmetic or Relational Operator	Description
=	If the compared expressions are equal, the packet matches.
!=	If the compared expressions are unequal, the packet matches.

Required Privilege Level trace
maintenance

List of Sample Output

monitor traffic count on page 32
monitor traffic detail count on page 32
monitor traffic extensive (Absolute Sequence) on page 33
monitor traffic extensive (Relative Sequence) on page 33
monitor traffic extensive count on page 33
monitor traffic interface on page 33
monitor traffic matching on page 34
monitor traffic (TX Matrix Plus Router) on page 34
monitor traffic (QFX3500 Switch) on page 35
monitor traffic matching icmp on page 35
monitor traffic matching IP protocol number on page 36
monitor traffic matching arp on page 36
monitor traffic matching port on page 37

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

monitor traffic count

```
user@host> monitor traffic count 2
listening on fxp0
04:35:49.814125  In my-server.home.net.1295 > my-server.work.net.telnet: . ack
4122529478 win 16798 (DF)
04:35:49.814185
Out my-server.work.net.telnet > my-server.home.net.1295: P
1:38(37) ack 0 win 17680 (DF) [tos 0x10]
```

monitor traffic detail count

```
user@host> monitor traffic detail count 2
listening on fxp0
04:38:16.265864  In my-server.home.net.1295 > my-server.work.net.telnet: . ack
4122529971 win 17678 (DF) (ttl 121, id 6812)
04:38:16.265926
Out my-server.work.net.telnet.telnet > my-server.home.net.1295: P 1:38(37) ack 0
 win 17680 (DF) [tos 0x10]  (ttl 6)
```

 Copyright © 2018, Juniper Networks, Inc.

monitor traffic extensive (Absolute Sequence)

```
user@host> monitor traffic extensive no-domain-names no-resolve no-timestamp count 20
matching "tcp" absolute-sequence
listening on fxp0
 In 203.0.113.193.179 > 192.168.4.227.1024: . 4042780859:4042780859(0)
ack 1845421797 win 16384 <nop,nop,timestamp 4935628 965951> [tos 0xc0]  (ttl )
 In 203.0.113.193.179 > 192.168.4.227.1024: P 4042780859:4042780912(53)
ack 1845421797 win 16384
<nop,nop,timestamp 4935628 965951>:
BGP [|BGP UPDAT)
In 192.168.4.227.1024 > 203.0.113.193.179:
P 1845421797:1845421852(55) ack 4042780912 win 16384 <nop,nop,timestamp 965951
4935628>: BGP [|BGP UPDAT)
...
```

monitor traffic extensive (Relative Sequence)

```
user@host> monitor traffic extensive no-domain-names no-resolve no-timestamp count 20
matching "tcp"
listening on fxp0
 In 172.24.248.221.1680 > 192.168.4.210.23: . 396159737:396159737(0)
ack 1664980689 win 17574 (DF) (ttl 121, id 50003)
Out 192.168.4.210.23 > 172.24.248.221.1680: P 1:40(39)
ack 0 win 17680 (DF) [tos 0x10]  (ttl 64, id 5394)
 In 203.0.113.193.179 > 192.168.4.227.1024: P 4042775817:4042775874(57)
ack 1845416593 win 16384 <nop,nop,timestamp 4935379 965690>: BGP [|BGP UPDAT)
...
```

monitor traffic extensive count

```
user@host>  monitor traffic extensive count 5 no-domain-names no-resolve
listening on fxp013:18:17.406933
In 192.168.4.206.2723610880 > 172.17.28.8.2049:
40 null (ttl 64, id 38367)13:18:17.407577
In 172.17.28.8.2049 > 192.168.4.206.2723610880:
reply ok 28 null (ttl 61, id 35495)13:18:17.541140
In 0:e0:1e:42:9c:e0 0:e0:1e:42:9c:e0 9000 60:
0000 0100 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 000013:18:17.591513
In 172.24.248.156.4139 > 192.168.4.210.23:
3556964918:3556964918(0)
ack 295526518 win 17601 (DF)
(ttl 121, id 14)13:18:17.591568
Out 192.168.4.210.23 >
172.24.248.156.4139: P 1:40(39)
ack 0 win 17680 (DF) [tos 0x10]
(ttl 64, id 52376)
```

monitor traffic interface

```
user@host> monitor traffic interface fxp0
listening on fxp0.0
18:17:28.800650  In server.home.net.723 > host1-0.lab.home.net.log
```

```
18:17:28.800733 Out host2-0.lab.home.net.login > server.home.net.7
18:17:28.817813  In host30.lab.home.net.syslog > host40.home0
18:17:28.817846  In host30.lab.home.net.syslog > host40.home0
...
```

monitor traffic matching

```
user@host> monitor traffic matching "net 192.168.1.0/24"
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is ON. Use <no-resolve> to avoid any reverse lookup delay.
Address resolution timeout is 4s.
Listening on fxp0, capture size 96 bytes

Reverse lookup for 192.168.1.255 failed (check DNS reachability).
Other reverse lookup failures will not be reported.
Use no-resolve to avoid reverse lookups on IP addresses.

21:55:54.003511  In IP truncated-ip - 18 bytes missing!
192.168.1.17.netbios-ns > 192.168.1.255.netbios-ns: UDP, length 50
21:55:54.003585 Out IP truncated-ip - 18 bytes missing!
192.168.1.17.netbios-ns > 192.168.1.255.netbios-ns: UDP, length 50
21:55:54.003864  In arp who-has 192.168.1.17 tell 192.168.1.9
...
```

monitor traffic (TX Matrix Plus Router)

```
user@host> monitor traffic
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is ON. Use <no-resolve> to avoid any reverse lookup delay.
Address resolution timeout is 4s.
Listening on em0, capture size 96 bytes
04:11:59.862121 Out IP truncated-ip - 25 bytes missing!
summit-em0.example.net.syslog > sv-log-01.example.net.syslog:
SYSLOG kernel.info, length: 57
04:11:59.862303
Out IP truncated-ip - 25 bytes missing!
summit-em0.example.net.syslog >
sv-log-02.example.net.syslog: SYSLOG kernel.info, length: 57
04:11:59.923948
In IP aj-em0.example.net.65235 >
summit-em0.example.net.telnet: .
ack 1087492766 win 33304 <nop,nop,timestamp 42366734 993490>
04:11:59.923983 Out IP truncated-ip - 232 bytes missing!
summit-em0.example.net.telnet > aj-em0.example.net.65235: P 1:241(240) ack 0 win
 33304
<nop,nop,timestamp 993590 42366734>
04:12:00.022900
In IP aj-em0.exmaple.net.65235 >
summit-em0.example.net.telnet: . ack 241 win 33304 <nop,nop,timestamp 42366834
993590>
04:12:00.141204
In IP truncated-ip - 40 bytes missing!
ipg-lnx-shell1.example.net.46182 > summit-em0.example.net.telnet: P
2950530356:2950530404(48) ack 485494987 win 63712
<nop,nop,timestamp 1308555294 987086>
04:12:00.141345
Out IP summit-em0.example.net.telnet >
ipg-lnx-shell1.example.net.46182: P 1:6(5)
ack 48 win 33304
```


Copyright © 2018, Juniper Networks, Inc.

```
<nop,nop,timestamp 993809 1308555294>
04:12:00.141572
In IP ipg-lnx-shell1.example.net.46182 >
summit-em0.example.net.telnet: .
ack 6 win 63712
<nop,nop,timestamp 1308555294 993809>
04:12:00.141597
Out IP summit-em0.example.net.telnet >
ipg-lnx-shell1.example.net.46182: P 6:10(4) ack 48 win 33304
<nop,nop,timestamp 993810 1308555294>
04:12:00.141821
In IP ipg-lnx-shell1.example.net.46182 >
summit-em0.exmaple.net.telnet: .
ack 10 win 63712 <nop,nop,timestamp 1308555294 993810>
04:12:00.141837 Out IP truncated-ip - 2 bytes missing!
summit-em0.example.net.telnet >
ipg-lnx-shell1.example.net.46182: P 10:20(10) ack 48 win 33304
<nop,nop,timestamp 993810 1308555294>
04:12:00.142072
In IP ipg-lnx-shell1.example.net.46182 >
summit-em0.example.net.telnet: . ack 20 win 63712
<nop,nop,timestamp 1308555294 993810>
04:12:00.142089 Out IP summit-em0.example.net.telnet >
ipg-lnx-shell1.example.net.46182: P 20:28(8) ack 48 win 33304 <nop,nop,timestamp
 993810 1308555294>
04:12:00.142321
In IP ipg-lnx-shell1.exmample.net.46182 >
summit-em0.englab.example.net.telnet: .
ack 28 win 63712 <nop,nop,timestamp 1308555294 993810>
04:12:00.142337
Out IP truncated-ip - 1 bytes missing!
summit-em0.example.net.telnet >
ipg-lnx-shell.example.net.46182: P 28:37(9) ack 48 win 33304 <nop,nop,timestamp
993810 1308555294>
...
```

monitor traffic (QFX3500 Switch)

```
user@switch> monitor traffic
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is ON. Use <no-resolve> to avoid any reverse lookup delay.
Address resolution timeout is 4s.
Listening on me4, capture size 96 bytes
Reverse lookup for 172.22.16.246 failed (check DNS reachability).
Other reverse lookup failures will not be reported.
Use <no-resolve> to avoid reverse lookups on IP addresses.
16:35:32.240873 Out IP truncated-ip - 112 bytes missing! labqfx-me0.example.net.ssh
 >
172.22.16.246.telefinder: P 4200727624:4200727756(132) ack 2889954831 win 65535
16:35:32.240900 Out IP truncated-ip - 176 bytes missing! labqfx-me0.example.net.ssh
 >
172.22.16.246.telefinder: P 132:328(196) ack 1 win 65535
...
```

monitor traffic matching icmp

```
user@host> monitor traffic matching "icmp" no-resolve
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is OFF.
Listening on me0, capture size 96 bytes
```

```
09:23:17.728737  In IP 172.19.10.9 > 10.10.211.93: ICMP echo request, id 1, seq
322, length 40
09:23:17.728780 Out IP 10.10.211.93 > 172.19.10.9: ICMP echo reply, id 1, seq
322, length 40
09:23:18.735848  In IP 172.19.10.9 > 10.10.211.93: ICMP echo request, id 1, seq
323, length 40
09:23:18.735891 Out IP 10.10.211.93 > 172.19.10.9: ICMP echo reply, id 1, seq
323, length 40
09:23:19.749732  In IP 172.19.10.9 > 10.10.211.93: ICMP echo request, id 1, seq
324, length 40
09:23:19.749775 Out IP 10.10.211.93 > 172.19.10.9: ICMP echo reply, id 1, seq
324, length 40
09:23:20.749747  In IP 172.19.10.9 > 10.10.211.93: ICMP echo request, id 1, seq
325, length 40
09:23:20.749791 Out IP 10.10.211.93 > 172.19.10.9: ICMP echo reply, id 1, seq
325, length 40
...
```

monitor traffic matching IP protocol number

```
user@host> monitor traffic matching "proto 89" no-resolve
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is OFF.
Listening on me0, capture size 96 bytes

13:06:14.700311  In IP truncated-ip - 16 bytes missing! 10.94.211.254 > 224.0.0.
5: OSPFv2, Hello, length 56
13:06:16.067010  In IP truncated-ip - 20 bytes missing! 10.94.211.102 > 224.0.0.
5: OSPFv2, Hello, length 60
13:06:16.287566  In IP truncated-ip - 20 bytes missing! 10.94.211.142 > 224.0.0.
5: OSPFv2, Hello, length 60
13:06:20.758500  In IP truncated-ip - 16 bytes missing! 10.200.211.254 > 224.0.0
.5: OSPFv2, Hello, length 56
13:06:24.309882  In IP truncated-ip - 20 bytes missing! 10.94.211.102 > 224.0.0.
5: OSPFv2, Hello, length 60
13:06:24.396699  In IP truncated-ip - 16 bytes missing! 10.94.211.254 > 224.0.0.
5: OSPFv2, Hello, length 56
13:06:25.067386  In IP truncated-ip - 20 bytes missing! 10.94.211.142 > 224.0.0.
5: OSPFv2, Hello, length 60
13:06:29.499988  In IP truncated-ip - 16 bytes missing! 10.200.211.254 > 224.0.0
.5: OSPFv2, Hello, length 56
13:06:32.858753  In IP truncated-ip - 20 bytes missing! 10.94.211.102 > 224.0.0.
5: OSPFv2, Hello, length 60
...
```

monitor traffic matching arp

```
user@host> monitor traffic matching “arp” no-resolve
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is OFF.
Listening on me0, capture size 96 bytes

11:57:54.664501  In arp who-has 10.10.213.109 (00:1f:d5:f3:28:30) tell 10.10.213.31
11:57:56.828387  In arp who-has 10.10.213.233 (00:24:9d:06:77:4f) tell 10.10.213.31
11:58:01.735803  In arp who-has 10.10.213.251 (88:e0:f4:1d:41:40) tell 10.10.213.31
11:58:04.663241  In arp who-has 10.10.213.254 tell 10.94.211.170
11:58:28.488191  In arp who-has 10.10.213.149 (00:e0:91:c2:ff:8d) tell 10.10.213.31
11:58:41.858612  In arp who-has 10.10.213.148 tell 10.94.211.254
11:58:42.621533  In arp who-has 10.10.213.254 (5f:5e:ac:79:49:81) tell 10.10.213.31
```


Copyright © 2018, Juniper Networks, Inc.

```
11:58:44.533391  In arp who-has 10.10.213.186 tell 10.94.211.254
11:58:45.170405  In arp who-has 10.10.213.186 tell 10.94.211.254
11:58:45.770512  In arp who-has 10.10.213.186 tell 10.94.211.254
```

monitor traffic matching port

```
user@host> monitor traffic matching "port 22" no-resolve
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is OFF.
Listening on me0, capture size 96 bytes

13:14:19.108089  In IP 192.0.2.22.56714 > 10.19.300.05.22: S
2210742342:2210742342(0) win 65535 <mss 1360,nop,wscale 7,nop,nop,sackOK>
13:14:19.108165 Out IP 10.19.300.05.22 > 192.0.2.22.56714: S 23075150:23075150(0)
 ack 2210742343 win 65535 <mss 1460,nop,wscale 1,sackOK,eol>
13:14:19.136883  In IP 192.0.2.22.56714 > 10.19.300.05.22: . ack 1 win 32768
13:14:19.231364 Out IP truncated-ip - 1 bytes missing! 10.19.300.05.22 >
172.29.102.9.56714: P 1:22(21) ack 1 win 33320
13:14:19.260174  In IP truncated-ip - 10 bytes missing! 192.0.2.22.56714 >
10.94.211.93.22: P 1:31(30) ack 22 win 32767
13:14:19.284865 Out IP truncated-ip - 964 bytes missing! 10.19.300.05.22 >
172.29.102.9.56714: P 22:1006(984) ack 31 win 33320
13:14:19.314549  In IP truncated-ip - 652 bytes missing! 192.0.2.22.56714 >
10.94.211.93.22: P 31:703(672) ack 1006 win 32760
13:14:19.414135 Out IP 10.19.300.05.22 > 192.0.2.22.56714: . ack 703 win 33320
13:14:19.443858  In IP 192.0.2.22.56714 > 10.19.300.05.22: P 703:719(16) ack 1006
 win 32760
13:14:19.467379 Out IP truncated-ip - 516 bytes missing! 10.19.300.05.22 >
172.29.102.9.56714: P 1006:1542(536) ack 719 win 33320
13:14:19.734097  In IP 192.0.2.22.56714 > 10.19.300.05.22: . ack 1542 win 32768
13:14:19.843574  In IP truncated-ip - 508 bytes missing! 192.0.2.22.56714 >
10.94.211.93.22: P 719:1247(528) ack 1542 win 32768
...
```

ping

List of Syntax

Syntax on page 38
Syntax (QFX Series) on page 38

Syntax

ping *host*
<bypass-routing>
<ce-ip *destination-ip-address* instance *routing-instance-name* source-ip *source-ip-address*>
<count *requests*>
<detail>
<do-not-fragment>
<inet | inet6>
<interface *source-interface*>
<interval *seconds*>
<logical-system *logical-system-name*>
<loose-source *value*>
<mac-address *mac-address*>
<no-resolve>
<pattern *string*>
<rapid>
<record-route>
<routing-instance *routing-instance-name*>
<size *bytes*>
<source *source-address*>
<strict >
<strict-source *value*.>
<tos *type-of-service*>
<ttl *value*>
<verbose>
<vpls *instance-name*>
<wait *seconds*>

Syntax (QFX Series)

ping *host*
<bypass-routing>
<count *requests*>
<detail>
<do-not-fragment>
<inet>
<interface *source-interface*>
<interval *seconds*>
<logical-system *logical-system-name*>
<loose-source *value*>
<mac-address *mac-address*>
<no-resolve>
<pattern *string*>
<rapid>
<record-route>
<routing-instance *routing-instance-name*>
<size *bytes*>
<source *source-address*>
<strict>
< strict-source *value*>
<tos *type-of-service*>

Copyright © 2018, Juniper Networks, Inc.

<ttl *value*>
<verbose>
<wait *seconds*>

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 the OCX Series.
ce-ip option introduced in Junos OS Release 17.3 for MX Series routers with MPC and MIC interfaces.

Description Check host reachability and network connectivity. The **ping** command sends Internet Control Message Protocol (ICMP) ECHO_REQUEST messages to elicit ICMP ECHO_RESPONSE messages from the specified host. Press Ctrl+c to interrupt a ping command.

Options ***host***—IP address or hostname of the remote system to ping.

bypass-routing—(Optional) Bypass the normal routing tables and send ping requests directly to a system on an attached network. If the system is not on a directly attached network, an error is returned. Use this option to ping a local system through an interface that has no route through it.

ce-ip *destination-ip-address* instance *routing-instance-name* source-ip *source-ip-address*—(MX Series routers with MPC and MIC interfaces only) (Optional) Check the connectivity information of customer edge (CE) devices, such as reachability, attachment points, and MAC addresses, from a provider edge (PE) device in a virtual private LAN service (VPLS), hierarchical VPLS (H-VPLS), and Ethernet VPN (EVPN) network. The **ce-ip** option is based on the LSP ping infrastructure, where the **ping** utility is extended to use the CE device IP address as the target host and the PE device loopback address as the source for a specific VPLS or EVPN routing instance.

destination-ip-address—IPv4 address of the CE device to ping.

instance *routing-instance-name*—Name of the VPLS or EVPN routing instance. The command output displays the connectivity information of the CE device based on the configured routing instance type.

source-ip *source-ip-address*—Loopback address of the PE device.

count *requests*—(Optional) Number of ping requests to send. The range of values is **1** through **2,000,000,000**. The default value is an unlimited number of requests.

detail—(Optional) Include in the output the interface on which the ping reply was received.

do-not-fragment—(Optional) Set the do-not-fragment (DF) flag in the IP header of the ping packets. For IPv6 packets, this option disables fragmentation.

NOTE: In Junos OS Release 11.1 and later, when issuing the **ping** command for an IPv6 route with the **do-not-fragment** option, the maximum ping packet size is calculated by subtracting 48 bytes (40 bytes for the IPV6 header and 8 bytes for the ICMP header) from the MTU. Therefore, if the ping packet size (including the 48-byte header) is greater than the MTU, the ping operation might fail.

inet—(Optional) Ping Packet Forwarding Engine IPv4 routes.

inet6—(Optional) Ping Packet Forwarding Engine IPv6 routes.

interface *source-interface*—(Optional) Interface to use to send the ping requests.

interval *seconds*—(Optional) How often to send ping requests. The range of values, in seconds, is **1** through infinity. The default value is **1**.

logical-system *logical-system-name*—(Optional) Name of logical system from which to send the ping requests.

Alternatively, enter the **set cli logical-system *logical-system-name*** command and then run the **ping** command. To return to the main router or switch, enter the **clear cli logical-system** command.

loose-source *value*—(Optional) Intermediate loose source route entry (IPv4). Open a set of values.

mac-address *mac-address*—(Optional) Ping the physical or hardware address of the remote system you are trying to reach.

no-resolve—(Optional) Do not attempt to determine the hostname that corresponds to the IP address.

pattern *string*—(Optional) Specify a hexadecimal fill pattern to include in the ping packet.

rapid—(Optional) Send ping requests rapidly. The results are reported in a single message, not in individual messages for each ping request. By default, five ping requests are sent before the results are reported. To change the number of requests, include the **count** option.

record-route—(Optional) Record and report the packet's path (IPv4).

routing-instance *routing-instance-name*—(Optional) Name of the routing instance for the ping attempt.

size *bytes*—(Optional) Size of ping request packets. The range of values, in bytes, is **0** through **65,468**. The default value is **56**, which is effectively 64 bytes because 8 bytes of ICMP header data are added to the packet.

Copyright © 2018, Juniper Networks, Inc.

source ***source-address***—(Optional) IP address of the outgoing interface. This address is sent in the IP source address field of the ping request. If this option is not specified, the default address is usually the loopback interface (**lo.0**).

strict—(Optional) Use the strict source route option (IPv4).

strict-source ***value***—(Optional) Intermediate strict source route entry (IPv4). Open a set of values.

tos ***type-of-service***—(Optional) Set the type-of-service (ToS) field in the IP header of the ping packets. The range of values is **0** through **255**.

If the device configuration includes the **dscp-code-point** ***value*** statement at the **[edit class-of-service host-outbound-traffic]** hierarchy level, the configured DSCP value overrides the value specified in this command option. In this case, the ToS field of ICMP echo request packets sent on behalf of this command carries the DSCP value specified in the **dscp-code-point** configuration statement instead of the value you specify in this command option.

ttl ***value***—(Optional) Time-to-live (TTL) value to include in the ping request (IPv6). The range of values is **0** through **255**.

verbose—(Optional) Display detailed output.

vpls ***instance-name***—(Optional) Ping the instance to which this VPLS belongs.

wait ***seconds***—(Optional) Maximum wait time, in seconds, after the final packet is sent. If this option is not specified, the default delay is **10** seconds. If this option is used without the count option, a default count of **5** packets is used.

Required Privilege Level

network

Related Documentation

- *Configuring Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages*
- *Pinging Customer Edge Device IP Address*

List of Sample Output

ping ce-ip <destination-ip-address> instance <routing-instance-name> source-ip <source-ip-address> (EVPN) on page 42
ping ce-ip <destination-ip-address> instance <routing-instance-name> source-ip <source-ip-address> (VPLS) on page 42
ping hostname on page 42
ping hostname rapid on page 42
ping hostname size count on page 42

Output Fields

When you enter this command, you are provided feedback on the status of your request. An exclamation point (**!**) indicates that an echo reply was received. A period (**.**) indicates that an echo reply was not received within the timeout period. An **x** indicates that an echo reply was received with an error code. These packets are not counted in the received packets count. They are accounted for separately.

Sample Output

ping ce-ip <destination-ip-address> instance <routing-instance-name> source-ip <source-ip-address> (EVPN)

```
user@host> ping ce-ip 10.0.0.4 instance foo source-ip 127.0.0.1
! -> PE5|foo|evpn|ge-0/0/2.100, 00:11:22:33:44:55:66:77:88:99|12:23:ab:98:34:05
! -> PE5|foo|evpn|ge-0/0/2.100, 00:11:22:33:44:55:66:77:88:99|12:23:ab:98:34:05
! -> PE5|foo|evpn|ge-0/0/2.100, 00:11:22:33:44:55:66:77:88:99|12:23:ab:98:34:05
! -> PE5|foo|evpn|ge-0/0/2.100, 00:11:22:33:44:55:66:77:88:99|12:23:ab:98:34:05
! -> PE5|foo|evpn|ge-0/0/2.100, 00:11:22:33:44:55:66:77:88:99|12:23:ab:98:34:05
--- ce-ip ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

ping ce-ip <destination-ip-address> instance <routing-instance-name> source-ip <source-ip-address> (VPLS)

```
user@host> ping ce-ip 10.0.0.4 instance foo source-ip 127.0.0.1
! -> PE2|foo|vpls|ge-0/0/2.100|12:23:ab:98:34:02
! -> PE2|foo|vpls|ge-0/0/2.100|12:23:ab:98:34:02
! -> PE2|foo|vpls|ge-0/0/2.100|12:23:ab:98:34:02
! -> PE2|foo|vpls|ge-0/0/2.100|12:23:ab:98:34:02
! -> PE2|foo|vpls|ge-0/0/2.100|12:23:ab:98:34:02
--- ce-ip ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

ping hostname

```
user@host> ping device1.example.com
PING device1.example.com (192.0.2.0): 56 data bytes
64 bytes from 192.0.2.0: icmp_seq=0 ttl=253 time=1.028 ms
64 bytes from 192.0.2.0: icmp_seq=1 ttl=253 time=1.053 ms
64 bytes from 192.0.2.0: icmp_seq=2 ttl=253 time=1.025 ms
64 bytes from 1192.0.2.0: icmp_seq=3 ttl=253 time=1.098 ms
64 bytes from 192.0.2.0: icmp_seq=4 ttl=253 time=1.032 ms
64 bytes from 192.0.2.0: icmp_seq=5 ttl=253 time=1.044 ms
^C [abort]
```

ping hostname rapid

```
user@host> ping device1.example.com rapid
PING device1.example.com (192.0.2.0): 56 data bytes
!!!!!
--- device1.example.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.956/0.974/1.025/0.026 ms
```

ping hostname size count

```
user@host> ping device1.example.com size 200 count 5
PING device1.example.com (192.0.2.0): 200 data bytes
208 bytes from 192.0.2.0: icmp_seq=0 ttl=253 time=1.759 ms
208 bytes from 192.0.2.0: icmp_seq=1 ttl=253 time=2.075 ms
208 bytes from 192.0.2.0: icmp_seq=2 ttl=253 time=1.843 ms
208 bytes from 192.0.2.0: icmp_seq=3 ttl=253 time=1.803 ms
208 bytes from 192.0.2.0: icmp_seq=4 ttl=253 time=17.898 ms

--- device1.example.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.759/5.075/17.898 ms
```


Copyright © 2018, Juniper Networks, Inc.

Copyright © 2018, Juniper Networks, Inc.

PART 2

Automation

- Configuring Automation on page 47
- Automation Configuration Statements on page 79

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 4

Configuring Automation

- Overview of Junos Automation Enhancements on page 47
- Overview of Python with Junos Automation Enhancements on page 48
- Understanding Automation Scripts Support on page 51
- How Commit Scripts Work on page 52
- Avoiding Potential Conflicts When Using Multiple Commit Scripts on page 58
- Overview of Generating Persistent or Transient Configuration Changes Using Commit Scripts on page 59
- Required Boilerplate for Commit Scripts on page 64
- How Op Scripts Work on page 66
- Required Boilerplate for Op Scripts on page 66
- Installing Junos OS Software with Junos Automation Enhancements on page 68
- Invoking the Python Interpreter on page 74
- Controlling the Execution of Commit Scripts on page 74
- Displaying Commit Script Output on page 77

Overview of Junos Automation Enhancements

The Junos Automation Enhancements are designed to support the increasing needs of large data centers for more automation and programmability.

- Features of the Junos Automation Enhancements on page 47

Features of the Junos Automation Enhancements

To use the Junos Automation Enhancements, you must install the software bundle that contains Enhanced Automation. The file name of the software bundle varies, depending on the switch. For example, for the QFX5200 switch, you would install an image with the filename **jinstall-qfx-5e-flex-*version*-domestic-signed.tgz**. This software bundle is identical to the other software bundle except that Veriexec is disabled, which enables you to run unsigned programs, such as programs that you develop with Python, Chef, and Puppet. The Junos Automation Enhancements include the following features:

- The factory default configuration is a Layer 3 configuration. (The standard default factory configuration on some devices series is Layer 2.)
- Safeguards ensure that you cannot overwrite essential Junos OS files, including system log notifications.
- The installation automatically sets up and reserves a 1 GB user partition on your system. You can use this partition to store your binaries and additional packages.
- The user partition is not overwritten when you upgrade or downgrade the software to a OS image that does not contain the automation enhancements.

  NOTE: **If you make changes to the user partition while performing a unified in-service software upgrade (unified ISSU), the changes might be lost.**

- The Python interpreter is included by default.
  - You can invoke Python directly from the shell. See "Invoking the Python Interpreter" on page 74.
  - Starting with Junos OS Release 14.1X53-D10, three Open Source Python modules are pre-installed in the **jinstall-qfx-5-flex-x.tgz** software bundle. See "Overview of Python with Junos Automation Enhancements" on page 48 for details.
- Chef for Junos OS and Puppet for Junos OS automation tools for provisioning and managing computer networking and storage resources are included.
  - For further information on Chef, see Chef for Junos Getting Started Guide.
  - For further information on Puppet, see Puppet for Junos OS Documentation.

  NOTE: **For full compatibility, you must use only Chef for Junos OS and Puppet for Junos OS rather than the standard FreeBSD versions of Chef and Puppet software.**

CAUTION: **Download additional third party packages at your own risk.**

Related Documentation

- Installing Junos OS Software with Junos Automation Enhancements on page 68
- Invoking the Python Interpreter on page 74

Overview of Python with Junos Automation Enhancements

Python is a programming language that lets you work more quickly and integrate your systems more effectively. The Python interpreter is included within the Junos operating system (Junos OS) **jinstall-qfx-5-flex-x.tgz** software bundle.

Copyright © 2018, Juniper Networks, Inc.

Python is also suitable as an extension language for customizable applications.

Starting with Junos OS Release 14.1X53-D10, the Open Source Python modules are pre-installed in the **jinstall-qfx-5-flex-x.tgz** software bundle. These modules are included:

- **ncclient**—Facilitates client scripting and application development through the NETCONF protocol. See http://ncclient.grnet.gr/0.3.2/ for documentation of some of the external APIs of the ncclient Python module. At the bottom of this list, see examples of usage of some of these APIs with sample scripts.
- **lxml**—Combines the speed and XML feature completeness of the C libraries libxml2 and libxslt with the simplicity of a native Python API. See http://lxml.de/ for documentation of some of the external APIs of the lxml Python module.
- **jinja2**—Serves as a fast, secure, designer-friendly templating language. See http://jinja.pocoo.org/docs/api/ for documentation of some of the external APIs of the jinja2 Python module.

Example usage of some of the APIs of the ncclient Python module follows:

* Example of "connect" and "command" API:

```
from ncclient import manager

def connect(host, port, user, password):
    conn = manager.connect(host=host,
            port=port,
            username=user,
            password=password,
            timeout=10,
            device_params = {'name':'junos'},
            hostkey_verify=False)

    print 'show version'
    print '*' * 30
    result = conn.command('show version', format='text')
    print result.xpath('output')[0].text

if __name__ == '__main__':
    connect('router', '22', 'netconf', 'juniper!')
```

* Example of "compare_configuration" API:

```
from ncclient import manager
from ncclient.xml_ import *

import time

def connect(host, port, user, password, source):
    conn = manager.connect(host=host,
            port=port,
            username=user,
            password=password,
            timeout=10,
            device_params = {'name':'junos'},
            hostkey_verify=False)

    compare_config = conn.compare_configuration(rollback=3)
    print compare_config.tostring
```

```
if __name__ == '__main__':
    connect('router', 830, 'netconf', 'juniper!', 'candidate')
```

* Example of "lock", "load_configuration", "validate", "commit", "discard_changes", "unlock" APIs:

```
from ncclient import manager
from ncclient.xml_ import *

import time

def connect(host, port, user, password, source):
    conn = manager.connect(host=host,
            port=port,
            username=user,
            password=password,
            timeout=10,
            device_params = {'name':'junos'},
            hostkey_verify=False)

    print 'locking configuration'
    lock = conn.lock()

    # build configuration element
    config = new_ele('system')
    sub_ele(config, 'host-name').text = 'foo'
    sub_ele(config, 'domain-name').text = 'bar'

    send_config = conn.load_configuration(config=config)
    print send_config.tostring

    check_config = conn.validate()
    print check_config.tostring

    compare_config = conn.compare_configuration()
    print compare_config.tostring

    print 'commit confirmed 300'
    #commit_config = conn.commit(confirmed=True, timeout='300')
    commit_config = conn.commit()
    print commit_config.tostring

    print 'sleeping for 5 sec...'
    time.sleep(5)

    discard_changes = conn.discard_changes()
    print discard_changes.tostring

    print 'unlocking configuration'
    unlock = conn.unlock()
    print unlock.tostring

if __name__ == '__main__':
    connect('router', 830, 'netconf', 'juniper!', 'candidate')
```

NOTE: For information on using Python, refer to your Python documentation.

Copyright © 2018, Juniper Networks, Inc.

Release History Table

Release	Description
14.1X53-D10	Starting with Junos OS Release 14.1X53-D10, the Open Source Python modules are pre-installed in the **jinstall-qfx-5-flex-x.tgz** software bundle.

Related Documentation

- Installing Junos OS Software with Junos Automation Enhancements on page 68
- Invoking the Python Interpreter on page 74
- FAQ: Junos Automation Enhancements

Understanding Automation Scripts Support

This document describes the support for the Junos OS automation scripts on the QFabric system Director devices.

Junos OS automation consists of a suite of tools used to automate operational and configuration tasks on network devices running Junos OS. The automation tools, which leverage the native XML capabilities of the Junos OS, include commit scripts, operation (op) scripts, event policies and event scripts, and macros.

NOTE: **Event policies and event scripts are not supported on the QFabric system at this time.**

The QFabric system supports Junos OS automation scripts that are written in Stylesheet Language Alternative Syntax (SLAX) version 1.0.

Commit scripts automate the commit process and enforce custom configuration rules. You can use commit scripts to generate specific errors and warnings, and customize configurations and configuration templates. When a candidate configuration is committed, it is inspected by each active commit script. If a configuration violates your custom rules and the scripts generate an error, the commit fails. If the commit is successful, any configuration changes (both transient and permanent) are incorporated into the active configuration before it is passed to the Director software, which distributes the configuration to all applicable QFabric system components, including Node devices and Node servers.

Op scripts automate operational and troubleshooting tasks. Op scripts can be executed manually from the Junos OS CLI or NETCONF XML management protocol, or they can be called from another script.

The QFabric system supports the following automation script features:

- Commit scripts and op scripts are supported.
- Scripts written in SLAX version 1 are supported.

Copyright © 2018, Juniper Networks, Inc.

- Scripts are configured and deployed from the Director group. Since there is more than one Director device in a Director group, scripts must be deployed by each Director device or deployed in the shared media space.
- Scripts are stored in the shared media at this location: **/pbdata/mgd_shared/*partition-ip*/var/db/scripts**. Under this directory, commit scripts are stored in the **commit** subdirectory, and op scripts are stored in the **op** subdirectory.
- Scripts are not stored in flash memory.

Related Documentation

- How Commit Scripts Work on page 52
- How Op Scripts Work on page 66
- Required Boilerplate for Commit Scripts on page 64
- Required Boilerplate for Op Scripts on page 66
- Controlling the Execution of Commit Scripts on page 74

How Commit Scripts Work

Commit scripts contain instructions that enforce custom configuration rules and are invoked during the commit process before the standard Junos OS validity checks are performed. You enable commit scripts by listing the names of one or more commit script files at the **[edit system scripts commit]** hierarchy level. These files must be added to the appropriate commit script directory on the device.

When you perform a commit operation, Junos OS executes each script in turn, passing the information in the post-inheritance candidate configuration to the scripts. The script inspects the configuration, performs the necessary tests and validations, and generates a set of instructions for performing certain actions. After all commit scripts have been executed, Junos OS then processes all of the scripts' instructions. If the commit process is not halted by a commit script, then Junos OS applies all the commit script changes and performs its final inspection of the checkout configuration.

NOTE: When committing a configuration that is inspected by one or more commit scripts, you might need to increase the amount of memory allocated to the commit scripts to accommodate the processing of large configurations. By default, the maximum amount of memory allocated for the data segment portion of an executed script is half of the total available memory of the system, up to a maximum value of 128 MB. To increase the maximum memory allocated for each executed commit script, configure the **max-datasize *size*** statement with an appropriate memory limit in bytes at the **[edit system scripts commit]** hierarchy level before committing the configuration.

Commit script actions can include generating error, warning, and system log messages. If errors are generated, the commit operation fails and the candidate configuration remains unchanged. This is the same behavior that occurs with standard commit errors. Commit

 Copyright © 2018, Juniper Networks, Inc.

scripts can also generate changes to the system configuration. Because the changes are loaded before the standard validation checks are performed, they are validated for correct syntax, just like statements already present in the configuration before the script is applied. If the syntax is correct, the configuration is activated and becomes the active, operational device configuration.

Commit scripts cannot make configuration changes to protected statements or within protected hierarchies. If a commit script attempts to modify or delete a protected statement or hierarchy, Junos OS issues a warning that the change cannot be made. Failure to modify a protected configuration element does not halt the commit script or the commit process.

The following sections discuss several important concepts related to the commit script input and output:

- Commit Script Input on page 53
- Commit Script Output on page 53
- Commit Scripts and the Junos OS Commit Model on page 55

Commit Script Input

The input for a commit script is the post-inheritance candidate configuration in Junos XML API format. The term *post-inheritance* means that all configuration group values have been inherited by their targets in the candidate configuration and that the inactive portions of the configuration have been removed. For more information about configuration groups, see the *CLI User Guide*.

When you issue the **commit** command, Junos OS automatically generates the candidate configuration in XML format and reads it into the management (mgd) process, at which time the input is evaluated by any commit scripts.

To display the XML format of the post-inheritance candidate configuration in the CLI, issue the **show | display commit-scripts view** command.

```
[edit]
user@host# show | display commit-scripts view
```

To display all configuration groups data, including script-generated changes to the groups, issue the **show groups | display commit-scripts** command.

```
[edit]
user@host# show groups | display commit-scripts
```

Commit Script Output

During the commit process, enabled commit scripts are executed sequentially, and the commit script output, or instruction set, is provided to Junos OS. After all commit scripts have been executed, Junos OS then processes all of the scripts' instructions.

Commit script actions can include generating warning, error, and system log messages, and making persistent and transient changes to the configuration. Table 8 on page 54 briefly outlines the various elements, templates, and functions that commit scripts can use to instruct Junos OS to perform various actions during the commit process. In some

cases, there are multiple ways to perform the same action. Because SLAX and XSLT scripts return a result tree, output elements like <syslog><message> that are present in SLAX and XSLT scripts are added directly into the result tree.

Table 8: Commit Scripts Actions and Output

Commit Script Output	SLAX / XSLT	Python
Generate a warning message to the committing user.	**<xnm:warning>**	jcs.emit_warning()
Generate an error message and cause the commit operation to fail.	**<xnm:error>**	jcs.emit_error()
Generate a system log message.	jcs:syslog() **<syslog><message>**	jcs.syslog()
Generate a persistent change to the configuration.	**<change>**	emit_change(*content*, 'change', *format*)
Generate a transient change to the configuration.	**<transient-change>**	emit_change(*content*, 'transient-change', *format*)

Generate a persistent change relative to the current context node as defined by an XPath expression.	**XSLT**
	`<xsl:call-template name="jcs:emit-change">`
	`<xsl:with-param name="content">`
	SLAX
	`call jcs:emit-change() {`
	`with $content = {  }`
	`}`
		–

Generate a transient change relative to the current context node as defined by an XPath expression.	**XSLT**
	`<xsl:call-template name="jcs:emit-change">`
	`<xsl:with-param name="tag"`
	`select="'transient-change'"/>`
	`<xsl:with-param name="content">`
	SLAX
	`call jcs:emit-change() {`
	`with $tag = "transient-change";`
	`with $content = {  }`
	`}`
		–

Copyright © 2018, Juniper Networks, Inc.

Table 8: Commit Scripts Actions and Output *(continued)*

Commit Script Output	SLAX / XSLT	Python

Generate a warning message in conjunction with a configuration change. You can use this set of tags to generate a notification that the configuration has been changed.	**XSLT**
	`<xsl:call-template name="jcs:emit-change">`
	`  <xsl:with-param name="message">`
	`  <xsl:text>`
	SLAX
	`call jcs:emit-change() {`
	`  with $message = {`
	`  expr "message";`
	`  }`
	`}`
		jcs.emit_warning()

Junos OS processes this output and performs the appropriate actions. Errors and warnings are passed back to the Junos OS CLI or to a Junos XML protocol client application. The presence of an error automatically causes the commit operation to fail. Persistent and transient changes are loaded into the appropriate configuration database.

To test the output of error, warning, and system log messages from commit scripts, issue the **commit check | display xml** command.

```
[edit]
user@host# commit check | display xml
```

To display a detailed trace of commit script processing, issue the **commit check | display detail** command.

```
[edit]
user@host# commit check | display detail
```

NOTE: System log messages do not appear in the trace output, so you cannot use the commit check operation to test script-generated system log messages. Furthermore, system log messages are written to the system log during a commit operation, but not during a commit check operation.

Related Documentation

- *Example: Protecting the Junos OS Configuration from Modification or Deletion*.
- *emit-change Template (SLAX and XSLT) and emit_change (Python)*

Commit Scripts and the Junos OS Commit Model

Junos OS uses a commit model to update the device's configuration. This model allows you to make a series of changes to a candidate configuration without affecting the operation of the device. When the changes are complete, you can commit the configuration. The commit operation saves the candidate configuration changes into the current configuration.

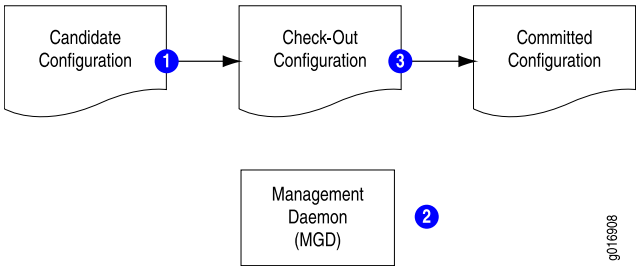
When you commit a set of changes in the candidate configuration, two methods are used to forward these changes to the current configuration:

- Standard commit model—Used when no commit scripts are active on the device.
- Commit script model—Incorporates commit scripts into the commit model.

Standard Commit Model

In the standard commit model, the management (mgd) process validates the candidate configuration based on standard Junos OS validation rules. If the configuration file is valid, it becomes the current active configuration. Figure 1 on page 56 and the accompanying discussion explain how the standard commit model works.

Figure 1: Standard Commit Model



In the standard commit model, the software performs the following steps:

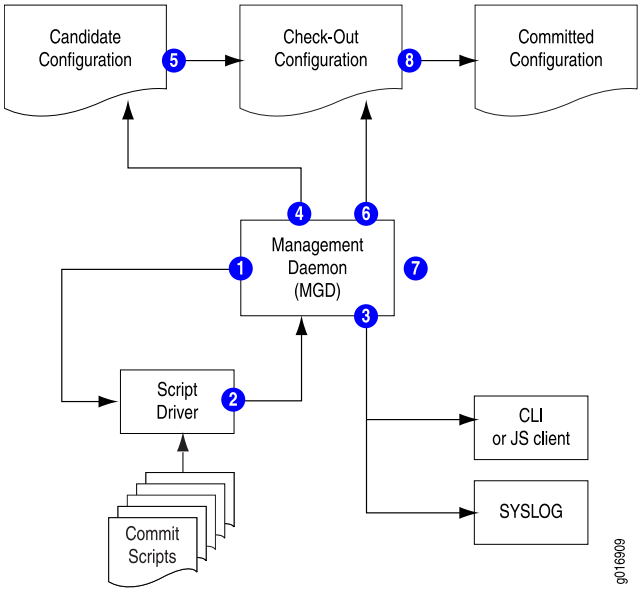
1. When the candidate configuration is committed, it is copied to become the checkout configuration.
2. The mgd process validates the checkout configuration.
3. If no error occurs, the checkout configuration is copied as the current active configuration.

Commit Model with Commit Scripts

When commit scripts are added to the standard commit model, the process becomes more complex. The mgd process first passes an XML-formatted checkout configuration to a script driver, which handles the verification of the checkout configuration by the commit scripts. When verification is complete, the script driver returns an *action file* to the mgd process. The mgd process follows the instructions in the action file to update the candidate and checkout configurations, issue messages to the CLI or client application, and write information to the system log as required. After processing the action file, the mgd process performs the standard Junos OS validation. Figure 2 on page 57 and the accompanying discussion explain this process.

Copyright © 2018, Juniper Networks, Inc.

Figure 2: Commit Model with Commit Scripts Added



In the commit script model, Junos OS performs the following steps:

1. When the candidate configuration is committed, the mgd process sends the XML-formatted candidate configuration to the script driver.
2. Each enabled commit script is invoked against the candidate configuration, and each script can generate a set of actions for the mgd process to perform. The actions are collected in an action file.
3. The mgd process performs the following actions for commit script error, warning, and system log messages in the action file:
   - error—The mgd process halts the commit process (that is, the commit operation fails), returns an error message to the CLI or Junos XML protocol client, and takes no further action.
   - warning—The mgd process forwards the message to the CLI or the Junos XML protocol client.
   - system log message—The mgd process forwards the message to the system log process.
4. If the action file includes any persistent changes, the mgd process loads the requested changes into the candidate configuration.
5. The candidate configuration is copied to become the checkout configuration.
6. If the action file includes any transient changes, the mgd process loads the requested changes into the checkout configuration.
7. The mgd process validates the checkout configuration.
8. If there are no validation errors, the checkout configuration is copied to become the current active configuration.

NOTE: Commit scripts cannot make configuration changes to protected statements or within protected hierarchies. If a commit script attempts to modify or delete a protected statement or hierarchy, Junos OS issues a warning that the change cannot be made. Failure to modify a protected configuration element does not halt the commit script or the commit process.

Changes that are made to the candidate configuration during the commit operation are not evaluated by the custom rules during that commit operation. However, persistent changes are maintained in the candidate configuration and are evaluated by the custom rules during subsequent commit operations. For more information about how commit scripts change the candidate configuration, see "Avoiding Potential Conflicts When Using Multiple Commit Scripts" on page 58.

Transient changes are never evaluated by the custom rules in commit scripts, because they are made to the checkout configuration only after the commit scripts have evaluated the candidate configuration and the candidate is copied to become the checkout configuration. To remove a transient change from the configuration, remove, disable, or deactivate the commit script (as discussed in *Controlling Execution of Commit Scripts During Commit Operations*), or comment out the code that generates the transient change.

For more information about differences between persistent and transient changes, see "Overview of Generating Persistent or Transient Configuration Changes Using Commit Scripts" on page 59.

Related Documentation

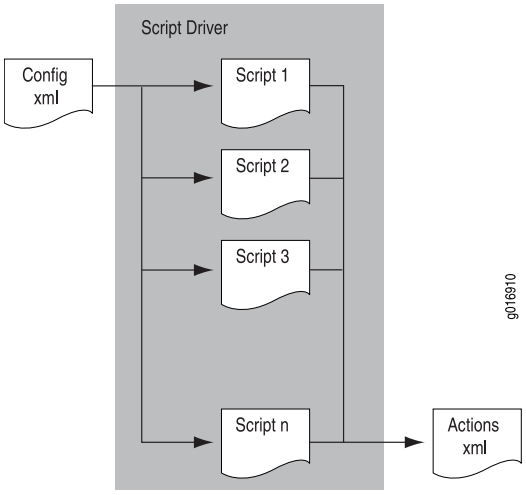
- *Controlling Execution of Commit Scripts During Commit Operations*
- Avoiding Potential Conflicts When Using Multiple Commit Scripts on page 58

Avoiding Potential Conflicts When Using Multiple Commit Scripts

When you use multiple commit scripts, each script evaluates the original candidate configuration file. Changes made by one script are not evaluated by the other scripts. This means that conflicts between scripts might not be resolved when the scripts are first applied to the configuration. The commit scripts are executed in the order they are listed at the **[edit system scripts commit]** hierarchy level, as illustrated in Figure 3 on page 59.

Copyright © 2018, Juniper Networks, Inc.

Figure 3: Configuration Evaluation by Multiple Commit Scripts



As an example of a conflict between commit scripts, suppose that commit script **A.xsl** is created to ensure that the device uses the domain name server with IP address 192.168.0.255. Later, the DNS server's address is changed to 192.168.255.255 and a second script, **B.xsl**, is added to check that the device uses the DNS server with that address. However, script **A.xsl** is not removed or disabled.

Because each commit script evaluates the original candidate configuration, the final result of executing both scripts **A.xsl** and **B.xsl** depends on which DNS server address is configured in the original candidate configuration. If the now outdated address of 192.168.0.255 is configured, script **B.xsl** changes it to 192.168.255.255. However, if the correct address of 192.168.255.255 is configured, script **A.xsl** changes it to the incorrect value 192.168.0.255.

As another example of a potential conflict between commit scripts, suppose that a commit script protects a hierarchy using the **protect** attribute. If a second commit script attempts to modify or delete the hierarchy or the statements within the hierarchy, Junos OS issues a warning during the commit process and prevents the configuration change.

Exercise care to ensure that you do not introduce conflicts between scripts like those described in the examples. As a method of checking for conflicts with persistent changes, you can issue two separate **commit** commands.

Related Documentation

- How Commit Scripts Work on page 52

Overview of Generating Persistent or Transient Configuration Changes Using Commit Scripts

Junos OS commit scripts enforce custom configuration rules. When a candidate configuration includes statements that you have decided must not be included in your configuration, or when the candidate configuration omits statements that you have

decided are required, commit scripts can automatically change the configuration and thereby correct the problem.

- Differences Between Persistent and Transient Changes on page 60
- Interaction of Configuration Changes and Configuration Groups on page 63
- Tag Elements and Templates for Generating Changes on page 63

Differences Between Persistent and Transient Changes

Configuration changes made by commit scripts can be *persistent* or *transient*.

A persistent change remains in the candidate configuration and affects routing operations until you explicitly delete it, even if you subsequently remove or disable the commit script that generated the change and reissue the **commit** command. In other words, removing the commit script does not cause a persistent change to be removed from the configuration.

A transient change, in contrast, is made in the *checkout configuration* but not in the candidate configuration. The checkout configuration is the configuration database that is inspected for standard Junos OS syntax just before it is copied to become the active configuration on the device. If you subsequently remove or disable the commit script that made the change and reissue the **commit** command, the change is no longer made to the checkout configuration and so does not affect the active configuration. In other words, removing the commit script effectively removes a transient change from the configuration.

A common use for transient changes is to eliminate the need to repeatedly configure and display well-known policies, thus allowing these policies to be enforced implicitly. For example, if MPLS must be enabled on every interface with an International Organization for Standardization (ISO) protocol enabled, the change can be transient, so that the repetitive or redundant configuration data need not be carried or displayed in the candidate configuration. Furthermore, transient changes allow you to write script instructions that apply the change only if a set of conditions is met.

Persistent and transient changes are loaded into the configuration in the same manner that the **load replace** configuration mode command loads an incoming configuration. When generating a persistent or transient change, adding the **replace="replace"** attribute to a configuration element produces the same behavior as a **replace:** tag in a **load replace** operation.

By default, Junos OS merges the incoming configuration and the candidate configuration. New statements and hierarchies are added, and conflicting statements are overridden. When generating a persistent or transient change, if you add the **replace="replace"** attribute to a configuration element, Junos OS replaces the existing configuration element with the incoming configuration element. If the **replace="replace"** attribute is added to a configuration element, but there is no existing element of the same name in the current configuration, the incoming configuration element is added into the configuration. Elements that do not have the **replace** attribute are merged into the configuration.

Persistent and transient changes are loaded before the standard Junos OS validation checks are performed. This means any configuration changes introduced by a commit

 Copyright © 2018, Juniper Networks, Inc.

script are validated for correct syntax. If the syntax is correct, the new configuration becomes the active, operational device configuration.

Protected elements in the configuration hierarchy cannot be modified or deleted by either a persistent or a transient change. If a commit script attempts to modify or delete a protected statement or hierarchy, Junos OS issues a warning that the change cannot be made, and proceeds with the commit.

Persistent and transient changes have several important differences, as described in Table 9 on page 61.

Table 9: Differences Between Persistent and Transient Changes

Persistent Changes	Transient Changes
You can represent a persistent change in commit scripts by using the **content** parameter in conjunction with a **tag** parameter that is set to 'change' inside a call to the **jcs:emit-change** template in SLAX and XSLT scripts or a call to the **jcs.emit_change** method in Python scripts. SLAX and XSLT commit scripts can also represent a persistent change by using the **<change>** tag.	You can represent a transient change in commit scripts with the **content** parameter in conjunction with the a **tag** parameter that is set to 'transient-change' inside a call to the **jcs:emit-change** template in SLAX and XSLT scripts or a call to the **jcs.emit_change** method in Python scripts. SLAX and XSLT commit scripts can also represent a transient change by using the **<transient-change>** tag.
You can use persistent changes to perform any Junos XML protocol operation, such as activate, deactivate, delete, insert (reorder), comment (annotate), and replace sections of the configuration.	Like persistent changes, you can use transient changes to perform any Junos XML protocol operation. However, some Junos XML protocol operations do not make sense to use with transient changes, such as generating comments and inactive settings.
Persistent changes are always loaded during the commit process if no errors are generated by any commit scripts or by the standard Junos OS validity check.	For transient changes to be loaded, you must include the **allow-transients** statement at the **[edit system scripts commit]** hierarchy level. If you enable a commit script that generates transient changes and you do not include the **allow-transients** statement in the configuration, the CLI generates an error message and the commit operation fails. You cannot use a commit script to generate the **allow-transients** statement. Like persistent changes, transient changes must pass the standard Junos OS validity check.
Persistent changes work like the **load replace** configuration mode command, and the change is added to the candidate configuration. When generating a persistent change, if you add the **replace="replace"** attribute to a configuration element, Junos OS replaces the existing element in the candidate configuration with the incoming configuration element. If there is no existing element of the same name in the candidate configuration, the incoming configuration element is added into the configuration. Elements that do not have the **replace** attribute are merged into the configuration.	Transient changes work like the **load replace** configuration mode command, and the change is added to the checkout configuration. When generating a transient change, if you add the **replace="replace"** attribute to a configuration element, Junos OS replaces the existing element in the checkout configuration with the incoming configuration element. If there is no existing element of the same name in the checkout configuration, the incoming configuration element is added into the configuration. Elements that do not have the **replace** attribute are merged into the configuration. Transient changes are not copied to the candidate configuration. For this reason, transient changes are not saved in the configuration if the associated commit script is deleted or deactivated.

Copyright © 2018, Juniper Networks, Inc.

Table 9: Differences Between Persistent and Transient Changes *(continued)*

Persistent Changes	Transient Changes
After a persistent change is committed, the software treats it like a change you make by directly editing and committing the candidate configuration. After the persistent changes are copied to the candidate configuration, they are copied to the checkout configuration. If the changes pass the standard Junos OS validity checks, the changes are propagated to the switch, router, or security device components.	Each time a transient change is committed, the software updates the checkout configuration database. After the transient changes pass the standard Junos OS validity checks, the changes are propagated to the device components.
After committing a script that causes a persistent change to be generated, you can view the persistent change by issuing the **show** configuration mode command: user@host# **show** This command displays persistent changes only, not transient changes.	After committing a script that causes a transient change to be generated, you can view the transient change by issuing the **show | display commit-scripts** configuration mode command: user@host# **show | display commit-scripts** This command displays both persistent and transient changes.
Persistent changes must conform to your custom configuration design rules as dictated by commit scripts. This does not become apparent until after a second commit operation because persistent changes are not evaluated by commit script rules on the current commit operation. The subsequent commit operation fails if the persistent changes do not conform to the rules imposed by the commit scripts configured during the first commit operation.	Transient changes are never tested by and do not need to conform to your custom rules. This is caused by the order of operations in the Junos OS commit model, which is explained in detail in "Commit Scripts and the Junos OS Commit Model" on page 55.
A persistent change remains in the configuration even if you delete, disable, or deactivate the commit script instructions that generated the change.	If you delete, disable, or deactivate the commit script instructions that generate a transient change, the change is removed from the configuration after the next commit operation. In short, if the associated instructions or the entire commit script is removed, the transient change is also removed.
As with direct CLI configuration, you can remove a persistent change by rolling back to a previous configuration that did not include the change and issuing the **commit** command. However, if you do not disable or deactivate the associated commit script, and the problem that originally caused the change to be generated still exists, the change is automatically regenerated when you issue another **commit** command.	You cannot remove a transient change by rolling back to a previous configuration.
You can alter persistent changes directly by editing the configuration using the CLI.	You cannot directly alter or delete a transient change by using the Junos OS CLI, because the change is not in the candidate configuration. To alter the contents of a transient change, you must alter the statements in the commit script that generates the transient change.

Copyright © 2018, Juniper Networks, Inc.

Interaction of Configuration Changes and Configuration Groups

Any configuration change you can make by directly editing the configuration using the Junos OS command-line interface (CLI) can also be generated by a commit script as a persistent or transient change. This includes values specified at a specific hierarchy level or in configuration groups. As with direct CLI configuration, values specified in the *target* override values inherited from a configuration group. The target is the statement to which you apply a configuration group by including the **apply-groups** statement.

If you define persistent or transient changes as belonging to a configuration group, the configuration groups are applied in the order you specify in the **apply-groups** statements, which you can include at any hierarchy level except the top level. You can also disable inheritance of a configuration group by including the **apply-groups-except** statement at any hierarchy level except the top level.

CAUTION: Each commit script inspects the postinheritance view of the configuration. If a candidate configuration contains a configuration group, be careful when using a commit script to change the related target configuration, because doing so might alter the intended inheritance from the configuration group.

Also be careful when using a commit script to change a configuration group, because the configuration group might be generated by an application that performs a load replace operation on the group during each commit operation.

For more information about configuration groups, see the *CLI User Guide*.

Tag Elements and Templates for Generating Changes

To generate persistent or transient changes in commit scripts, SLAX and XSLT scripts can use the **jcs:emit-change** template, and Python scripts can use the **jcs.emit_change** method. The **jcs:emit-change** template and **jcs.emit_change** method implicitly include **<change>** and **<transient-change>** XML elements. SLAX and XSLT scripts can also generate changes by including the **<change>** and **<transient-change>** elements directly in the commit script. Using the **jcs:emit-change** template in SLAX and XSLT scripts allows you to set the hierarchical context of the change once rather than multiple times. In Python scripts, the **jcs.emit_change** method requires that the configuration data for the requested change include the full configuration path representing all levels of the configuration hierarchy formatted as an XML string.

The **<change>** and **<transient-change>** elements are similar to the **<load-configuration>** operation defined by the Junos XML management protocol. The possible contents of the **<change>** and **<transient-change>** elements are the same as the contents of the **<configuration>** tag element used in the Junos XML protocol operation **<load-configuration>**. For complete details about the **<load-configuration>** element, see the *Junos XML Management Protocol Developer Guide*.

Related Documentation

- *Generating a Persistent or Transient Configuration Change in SLAX and XSLT Commit Scripts*
- *SLAX and XSLT Commit Script Tag Elements to Use When Generating Persistent and Transient Configuration Changes*

Required Boilerplate for Commit Scripts

Junos OS commit scripts can be written in Extensible Stylesheet Language Transformations (XSLT), Stylesheet Language Alternative syntaX (SLAX), or Python. Commit scripts must include the necessary boilerplate required for that script language for both basic script functionality as well as any optional functionality used within the script such as the Junos OS extension functions and named templates. This topic provides standard boilerplate that can be used in XSLT, SLAX, and Python scripts.

SLAX and XSLT commit scripts are based on Junos XML and Junos XML protocol tag elements. Like all XML elements, angle brackets enclose the name of a Junos XML or Junos XML protocol tag element in its opening and closing tags. This is an XML convention, and the brackets are a required part of the complete tag element name. They are not to be confused with the angle brackets used in the documentation to indicate optional parts of Junos OS CLI command strings.

XSLT Boilerplate for Commit Scripts

The XSLT commit script boilerplate is as follows:

```
1    <?xml version="1.0" standalone="yes"?>
2    <xsl:stylesheet version="1.0"
3        xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
4        xmlns:junos="http://xml.juniper.net/junos/*/junos"
5        xmlns:xnm="http://xml.juniper.net/xnm/1.1/xnm"
6        xmlns:jcs="http://xml.juniper.net/junos/commit-scripts/1.0">
7        <xsl:import href="../import/junos.xsl"/>

8        <xsl:template match="configuration">
             <!-- ... insert your code here ... -->
9        </xsl:template>
10   </xsl:stylesheet>
```

Line 1 is the Extensible Markup Language (XML) processing instruction (PI). This PI specifies that the code is written in XML using version 1.0. The XML PI, if present, must be the first noncomment token in the script file.

```
1    <?xml version="1.0"?>
```

Line 2 opens the style sheet and specifies the XSLT version as 1.0.

```
2    <xsl:stylesheet version="1.0"
```

Lines 3 through 6 list all the namespace mappings commonly used in commit scripts. Not all of these prefixes are used in this example, but it is not an error to list namespace mappings that are not referenced. Listing all namespace mappings prevents errors if the mappings are used in later versions of the script.

```
3        xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
4        xmlns:junos="http://xml.juniper.net/junos/*/junos"
5        xmlns:xnm="http://xml.juniper.net/xnm/1.1/xnm"
6        xmlns:jcs="http://xml.juniper.net/junos/commit-scripts/1.0">
```


Copyright © 2018, Juniper Networks, Inc.

Line 7 is an XSLT import statement. It loads the templates and variables from the file referenced as **../import/junos.xsl**, which ships as part of the Junos OS. The **junos.xsl** file contains a set of named templates you can call in your scripts. These named templates are discussed in *Understanding Named Templates in Junos OS Automation Scripts*.

```
7        <xsl:import href="../import/junos.xsl"/>
```

Line 8 defines a template that matches the **<configuration>** element, which is the node selected by the **<xsl:template match="/">** template, contained in the **junos.xsl** import file. The **<xsl:template match="configuration">** element allows you to exclude the **/configuration/** root element from all XPath expressions in the script and begin XPath expressions with the top Junos OS hierarchy level. For more information, see *XPath Overview*.

```
8        <xsl:template match="configuration">
```

Add your code between Lines 8 and 9.

Line 9 closes the template.

```
9        </xsl:template>
```

Line 10 closes the style sheet and the commit script.

```
10    </xsl:stylesheet>
```

SLAX Boilerplate for Commit Scripts

The corresponding SLAX commit script boilerplate is as follows:

```
version 1.0;
ns junos = "http://xml.juniper.net/junos/*/junos";
ns xnm = "http://xml.juniper.net/xnm/1.1/xnm";
ns jcs = "http://xml.juniper.net/junos/commit-scripts/1.0";
import "../import/junos.xsl";

match configuration {
   /*
    * insert your code here
    */
}
```

Python Boilerplate for Commit Scripts

Python commit scripts do not have a required boilerplate, but they must import any objects that are used in the script. Python automation scripts import the **Junos_Context** dictionary when the script must access information about the script execution environment. The **Junos_Configuration** object is required when the commit script must read and manipulate the post-inheritance candidate configuration. Python automation scripts that include the **import jcs** statement can use Junos OS extension functions and Junos OS named template functionality in the script.

```
from junos import Junos_Context
from junos import Junos_Configuration
import jcs

if __name__ == '__main__':
```

Python automation scripts do not need to include an interpreter directive line (**#!/usr/bin/env python**) at the start of the script. However, the program will still execute correctly if one is present.

Related Documentation

- *Understanding Extension Functions in Junos OS Automation Scripts*
- *Understanding Named Templates in Junos OS Automation Scripts*
- *Global Parameters and Variables in Junos OS Automation Scripts*

How Op Scripts Work

Op scripts execute Junos OS operational commands and inspect the resulting output. After inspection, op scripts can manipulate the output or automatically correct errors within the device running Junos OS based on this output.

You enable op scripts by listing the filenames of one or more op script files within the **[edit system scripts op]** hierarchy level. To execute local op scripts, you must add the files to the appropriate op script directory on the device. For more information about op script file directories, see *Storing and Enabling Scripts*. Once added to the device, op scripts are invoked from the command line, using the **op *filename*** command.

You can also store and execute op scripts from a remote site. Remote op scripts are invoked from the command line using the **op url *url*** command. For more information about executing remote op scripts, see *Executing an Op Script from a Remote Site*.

You can use op scripts to generate changes to the device configuration. Because the changes are loaded before the standard validation checks are performed, they are validated for correct syntax, just like statements already present in the configuration before the script is applied. If the syntax is correct, the configuration is activated and becomes the active, operational device configuration.

Related Documentation

- *Op Script Overview*
- *Executing an Op Script*
- *Executing an Op Script from a Remote Site*

Required Boilerplate for Op Scripts

Junos OS op scripts can be written in Extensible Stylesheet Language Transformations (XSLT), Stylesheet Language Alternative syntaX (SLAX), or Python. Op scripts must include the necessary boilerplate required for that script language for both basic script functionality as well as any optional functionality used within the script such as the Junos OS extension functions and named templates. This topic provides standard boilerplate that can be used in XSLT, SLAX, and Python scripts.

SLAX and XSLT op scripts are based on Junos XML and Junos XML protocol tag elements. Like all XML elements, angle brackets enclose the name of a Junos XML or Junos XML protocol tag element in its opening and closing tags. This is an XML convention, and the brackets are a required part of the complete tag element name. They are not to be confused with the angle brackets used in the documentation to indicate optional parts of Junos OS CLI command strings.

Copyright © 2018, Juniper Networks, Inc.

XSLT Boilerplate for Op Scripts

The XSLT op script boilerplate is as follows:

```
1    <?xml version="1.0" standalone="yes"?>
2    <xsl:stylesheet version="1.0"
3        xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
4        xmlns:junos="http://xml.juniper.net/junos/*/junos"
5        xmlns:xnm="http://xml.juniper.net/xnm/1.1/xnm"
6        xmlns:jcs="http://xml.juniper.net/junos/commit-scripts/1.0">
7        <xsl:import href="../import/junos.xsl"/>

8        <xsl:template match="/">
9            <op-script-results>
               <!-- ... insert your code here ... -->
10           </op-script-results>
11       </xsl:template>
       <!-- ... insert additional template definitions here ... -->
12   </xsl:stylesheet>
```

Line 1 is the Extensible Markup Language (XML) processing instruction (PI), which marks this file as XML and specifies the version of XML as 1.0. The XML PI, if present, must be the first non-comment token in the script file.

```
1    <?xml version="1.0"?>
```

Line 2 opens the style sheet and specifies the XSLT version as 1.0.

```
2    <xsl:stylesheet version="1.0"
```

Lines 3 through 6 list all the namespace mappings commonly used in operation scripts. Not all of these prefixes are used in this example, but it is not an error to list namespace mappings that are not referenced. Listing all namespace mappings prevents errors if the mappings are used in later versions of the script.

```
3        xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
4        xmlns:junos="http://xml.juniper.net/junos/*/junos"
5        xmlns:xnm="http://xml.juniper.net/xnm/1.1/xnm"
6        xmlns:jcs="http://xml.juniper.net/junos/commit-scripts/1.0">
```

Line 7 is an XSLT import statement. It loads the templates and variables from the file referenced as **../import/junos.xsl**, which ships as part of Junos OS (in the file **/usr/libdata/cscript/import/junos.xsl**). The **junos.xsl** file contains a set of named templates you can call in your scripts. These named templates are discussed in *Understanding Named Templates in Junos OS Automation Scripts* .

```
7        <xsl:import href="../import/junos.xsl"/>
```

Line 8 defines a template that matches the **</>** element. The **<xsl:template match="/">** element is the root element and represents the top level of the XML hierarchy. All XPath expressions in the script must start at the top level. This allows the script to access all possible Junos XML and Junos XML protocol remote procedure calls (RPCs). For more information, see *XPath Overview*.

```
8        <xsl:template match="/">
```

After the **<xsl:template match="/">** tag element, the **<op-script-results>** and **</op-script-results>** container tags must be the top-level child tags, as shown in Lines 9 and 10.

```
9            <op-script-results>
               <!-- ... insert your code here ... -->
10           </op-script-results>
```

Line 11 closes the template.

```
11        </xsl:template>
```

Between Line 11 and Line 12, you can define additional XSLT templates that are called from within the **<xsl:template match="/">** template.

Line 12 closes the style sheet and the op script.

```
12    </xsl:stylesheet>
```

SLAX Boilerplate for Op Scripts

The corresponding SLAX op script boilerplate is as follows:

```
version 1.0;

ns junos = "http://xml.juniper.net/junos/*/junos";
ns xnm = "http://xml.juniper.net/xnm/1.1/xnm";
ns jcs = "http://xml.juniper.net/junos/commit-scripts/1.0";
import "../import/junos.xsl";

match / {
    <op-script-results> {
        /*
            * Insert your code here
        */
    }
}
```

Python Boilerplate for Op Scripts

Python op scripts do not have a required boilerplate, but they must import any objects that are used in the script. Python automation scripts import the **Junos_Context** dictionary when the script must access information about the script execution environment. Python automation scripts that include the **import jcs** statement can use Junos OS extension functions and Junos OS named template functionality in the script. If the script uses Junos PyEZ functionality, it must import the necessary classes from the **jnpr.junos** module.

```
from junos import Junos_Context
from jnpr.junos import Device
import jcs

if __name__ == '__main__':
```

Python automation scripts do not need to include an interpreter directive line (**#!/usr/bin/env python**) at the start of the script. However, the program will still execute correctly if one is present.

Related Documentation

- *Understanding Extension Functions in Junos OS Automation Scripts*
- *Understanding Named Templates in Junos OS Automation Scripts*
- *Global Parameters and Variables in Junos OS Automation Scripts*

Installing Junos OS Software with Junos Automation Enhancements

Junos operating system (Junos OS) with Junos Automation Enhancements is a full-featured version of Junos OS with Veriexec disabled, which can only be installed on supported devices.

 Copyright © 2018, Juniper Networks, Inc.

NOTE: **You must install the jinstall-qfx-5-flex-x.tgz software bundle in order to use the automation enhancements.**

Before you install software, download the Junos OS jinstall-qfx-5-flex-x.tgz software bundle. For information on downloading and accessing the files, see *Upgrading Software*.

BEST PRACTICE: **Before you install the software, back up any critical files in /var/home.** For more information regarding how to back up critical files, contact Customer Support at https://www.juniper.net/support.

Install the software:

1. Execute the **request system software add** command with the **validate** option:

   - If the installation package resides locally on the switch, execute the **request system software add validate *pathname source* reboot** command, using the following format:

     ```
     user@switch> request system software add validate /var/tmp/jinstall-qfx-5-flex-x.tgz
     reboot
     ```

   - If the installation package resides remotely, execute the **request system software add validate *pathname source* reboot** command, using the following format:

     ```
     user@switch> request system software add validate
     ftp://ftpserver/directory/jinstall-qfx-5-flex-x.tgz reboot
     ```

2. After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

   ```
   user@switch> show version
   root@qfx5100-24q-et013> show version
   fpc0:
   --------------------------------------------------------------------------
   Hostname: qfx5100-24q-et013
   Model: qfx5100-24q-2p
   JUNOS Base OS Software Suite [13.2X51-D20]
   JUNOS Base OS boot [13.2X51-D20]
   JUNOS Crypto Software Suite [13.2X51-D20]
   JUNOS Online Documentation [13.2X51-D20]
   JUNOS Kernel Software Suite [13.2X51-D20]
   JUNOS Packet Forwarding Engine Support (qfx-x86-32) [13.2X51-D20]
   JUNOS Routing Software Suite [13.2X51-D20]
   JUNOS Enterprise Software Suite [13.2X51-D20]
   JUNOS py-base-i386 [13.2X51-D20]
   Puppet on Junos [2.7.19_1.junos.i386]
   Ruby Interpreter [11.10.4_1.junos.i386]
   Chef [11.10.4_1.junos.i386]
   junos-ez-stdlib [11.10.4_1.junos.i386]
   JUNOS Host Software [13.2X51-D20]
   JUNOS for Automation Enhancement
   ```


Copyright © 2018, Juniper Networks, Inc.

NOTE: If you are upgrading a device from standard Junos OS to use Junos Automation Enhancements and you are *not* loading the new factory default configuration, you need to use the following procedure.

To upgrade an existing device from standard Junos to use Junos Automation Enhancements:

1. Edit your existing Junos OS configuration to include the following configuration statements:

```
[edit]
user@switch# set system extensions providers juniper license-type juniper
deployment-scope commercial
user@switch# set system extensions providers chef license-type juniper
deployment-scope commercial
```

NOTE: The factory default configuration of the QFX5100 switch jinstall-qfx-5-flex-x.tgz software bundle is a Layer 3 configuration, whereas the factory default configuration for QFX5100 switch software bundles is a Layer 2 configuration. Therefore, if you are running the jinstall-qfx-5-flex-x.tgz software bundle on a QFX5100 switch and you use the **load factory-default** command, the resulting factory default configuration is set up for Layer 3 interfaces.

This is the factory default configuration for QFX5100 switch jinstall-qfx-5-flex-x.tgz software bundle:

```
user@switch> show configuration

system syslog user * any emergency
system syslog file messages any notice
system syslog file messages authorization info
system syslog file interactive-commands interactive-commands any
system extensions providers juniper license-type juniper deployment-scope
commercial
system extensions providers chef license-type juniper deployment-scope commercial
system commit factory-settings reset-virtual-chassis-configuration
system commit factory-settings reset-chassis-lcd-menu
system processes app-engine-virtual-machine-management-service traceoptions level
 notice
system processes app-engine-virtual-machine-management-service traceoptions flag
 all
interfaces et-0/0/0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/0:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/0:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/0:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/0:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/1:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/1:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/1:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/1:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
```

```
interfaces et-0/0/2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/2:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/2:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/2:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/2:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/3:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/3:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/3:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/3:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/4 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/4:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/4:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/4:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/4:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/5 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/5:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/5:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/5:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/5:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/6 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/6:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/6:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/6:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/6:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/7 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/7:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/7:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/7:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/7:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/8 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/8:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/8:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/8:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/8:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/9 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/9:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/9:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/9:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/9:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/10 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/10:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/10:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/10:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/10:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/11 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/11:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/11:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/11:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/11:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/12 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/12:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/12:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/12:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/12:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/13 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/13:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/13:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/13:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/13:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/14 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
```


Copyright © 2018, Juniper Networks, Inc.

```
interfaces xe-0/0/14:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/14:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/14:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/14:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/15 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/15:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/15:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/15:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/15:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/16 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/16:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/16:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/16:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/16:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/17 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/17:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/17:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/17:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/17:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/18 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/18:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/18:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/18:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/18:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/19 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/19:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/19:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/19:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/19:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/20 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/20:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/20:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/20:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/20:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/21 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/21:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/21:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/21:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/21:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/22 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/22:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/22:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/22:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/22:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/0/23 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/23:0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/23:1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/23:2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces xe-0/0/23:3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/1/0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/1/1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/1/2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/1/3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/2/0 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/2/1 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/2/2 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
interfaces et-0/2/3 unit 0 family inet dhcp vendor-id Juniper-qfx5100-24q-2p
forwarding-options storm-control-profiles default all
protocols lldp interface all
protocols lldp-med interface all
```

```
protocols igmp-snooping vlan default
vlans default vlan-id 1
```

Related Documentation

- Overview of Junos Automation Enhancements on page 47

Invoking the Python Interpreter

The Python interpreter is available by default with the Junos Automation Enhancements. You can invoke Python by entering the **python** command at the shell script.

To invoke the Python interpreter:

1. Start the shell interface:

   ```
   user@switch> start shell
   ```

2. Enter the **python** command without any parameters:

   ```
   % python
   ```

NOTE: The Python interpreter is designated with the prompt >>> at the beginning of a line or ... to indicate the continuation of a line.

Related Documentation

- Overview of Python with Junos Automation Enhancements on page 48
- Overview of Junos Automation Enhancements on page 47
- Installing Junos OS Software with Junos Automation Enhancements on page 68
- FAQ: Junos Automation Enhancements

Controlling the Execution of Commit Scripts

This document describes the tasks that affect the way commit scripts are executed. In the QFabric system, commit scripts are stored in the in the **/pbdata/mgd_shared/*partition-ip*/var/db/scripts/commit** directory that is shared among Director devices in a Director group.

To determine which commit scripts are currently enabled on the QFabric system, use the **show** command to display the files included at the **[edit system scripts commit]** hierarchy level. To ensure that the enabled files are on the device, list the contents of the

Copyright © 2018, Juniper Networks, Inc.

/pbdata/mgd_shared/*partition-ip*/var/db/scripts/commit directory using the **file list** operational mode command.

See the following tasks:

- Enabling Commit Scripts to Execute on page 75
- Removing Commit Scripts from the Configuration on page 75
- Deactivating Commit Scripts on page 76
- Activating Inactive Commit Scripts on page 77

Enabling Commit Scripts to Execute

The commit operation requires that all scripts be included in configuration at the **[edit system scripts commit file]** hierarchy level for all QFabric Director devices.

If you need to temporarily remove a script from a commit operation but do not want to remove it from the configuration permanently, you may configure the **optional** statement at the **[edit system scripts commit file *filename*]** hierarchy level to enable the commit operation to succeed even if a script is missing from the commit script directory.

CAUTION: When you include the **optional** statement at the **[edit system scripts commit file *filename*]** hierarchy level, no error message is generated during the commit operation if the file does not exist. As a result, you might not be aware that a script has not been executed as expected.

The filename of a commit script written in SLAX must include the **.slax** extension for the script to be executed.

To enable a commit script to execute during a commit operation:

1. Ensure that the commit script is located in the correct directory: **/pbdata/mgd_shared/*partition-ip*/var/db/scripts/commit** directory on the Director device.

2. Configure the commit script.

```
[edit system scripts commit]
user@switch# set file filename <optional>
```

3. Commit the configuration.

```
[edit system scripts commit]
user@switch# top
[edit]
user@switch# commit
```

Removing Commit Scripts from the Configuration

You can prevent commit scripts from executing during a commit operation by removing the scripts from the commit directory in the configuration.

NOTE: You can also deactivate a script using the **deactivate** statement instead of removing it from the configuration. Deactivated scripts may be reactivated later.

To prevent a commit script from executing during a commit operation:

1. Delete the commit script file from the commit directory in the configuration.

   [edit system scripts commit]
   user@switch# **delete file** ***filename***

2. Commit the configuration.

   [edit system scripts commit]
   user@switch# **top**
   [edit]
   user@switch# **commit**

3. Remove the commit script from the **/pbdata/mgd_shared/** directory on the Director device.

   BEST PRACTICE: Although removing the commit script is not necessary, we recommend deleting unused files from the system.

Deactivating Commit Scripts

Deactivating a commit script results in its being marked as inactive in the configuration. The script is not executed during the commit operation, but you can reactivate the script by using the **activate** statement.

To deactivate the commit script:

1. Deactivate the script.

   [edit]
   user@switch **deactivate system scripts commit file** ***filename***

2. Commit your changes.

   [edit]
   user@switch# **commit**

3. Verify that the commit script is deactivated.

   [edit]
   user@switch# **show system scripts commit**
   inactive: file mycommit.slax

Copyright © 2018, Juniper Networks, Inc.

Activating Inactive Commit Scripts

Deactivating a commit script results in its being marked as inactive in the configuration and is therefore not executed during the commit operation.

To activate an inactive commit script:

1. Activate the script.

   [edit]
   user@switch# **activate system scripts commit file** ***filename***

2. Commit your changes.

   [edit]
   user@switch# **commit**

See Also

- Understanding Automation Scripts Support on page 51

Displaying Commit Script Output

Table 10 on page 77 summarizes the Junos OS command-line interface (CLI) commands you can use to monitor and troubleshoot commit scripts. For more information about the **cscript.log** file, see *Tracing Commit Script Processing*.

NOTE: Tracing commit script processing, including the **cscript.log** file, is not supported on the QFX3000-G QFabric system.

Table 10: Commit Script Configuration and Operational Mode Commands

Task	Command
Configuration Mode Commands	
Display errors and warnings generated by commit scripts.	**commit** or **commit check**
Display detailed information about the commit operation and commit script execution.	**commit | display detail**
Display the underlying Extensible Markup Language (XML) data.	**commit | display xml**
Display the postinheritance contents of the configuration database. This view includes transient changes, but does not include changes made in configuration groups.	**show | display commit-scripts**
Display the postinheritance contents of the configuration database. This view excludes transient changes.	**show | display commit-scripts no-transients**

Table 10: Commit Script Configuration and Operational Mode Commands *(continued)*

Task	Command
Display the postinheritance configuration in XML format. This is the configuration format that each commit script receives as input. Viewing the configuration in XML format can be helpful when you are writing XML Path Language (XPath) expressions and configuration element tags.	**show | display commit-scripts view**
Display the postinheritance configuration in XML format, but exclude transient changes.	**show | display commit-scripts view | display commit-scripts no-transients**
Display all configuration groups data, including script-generated changes to the groups.	**show groups | display commit-scripts**
Display a particular configuration group, including script-generated changes to the group.	**show groups *group-name* | display commit-scripts**
Operational Mode Commands	
Display logging data associated with all commit script processing.	**show log cscript.log**
Display processing for only the most recent commit operation.	**show log cscript.log | last**
Display processing for script errors.	**show log cscript.log | match error**
Display processing for a particular script.	**show log cscript.log | match *filename***

Related Documentation

- *Tracing Commit Script Processing*

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 5

Automation Configuration Statements

- allow-transients on page 80
- apply-macro on page 81
- checksum on page 82
- command on page 83
- commit on page 84
- description on page 85
- direct-access on page 85
- file (Commit Scripts) on page 86
- file (Op Scripts) on page 87
- no-allow-url (Op Scripts) on page 88
- op on page 89
- optional on page 90
- refresh (Commit Scripts) on page 91
- refresh (Op Scripts) on page 92
- refresh-from (Commit Scripts) on page 93
- refresh-from (Op Scripts) on page 94
- scripts on page 95
- source (Commit Scripts) on page 97
- source (Op Scripts) on page 98

Copyright © 2018, Juniper Networks, Inc.

allow-transients

Syntax allow-transients;

Hierarchy Level [edit system scripts commit]

Release Information Statement introduced in Junos OS Release 7.4.
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 For Junos OS commit scripts, enable transient configuration changes to be committed.

Default Transient changes are disabled by default. If you do not include the **allow-transients** statement, and an enabled script generates transient changes, the command-line interface (CLI) generates an error message and the commit operation fails.

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

Related Documentation

- *Generating a Persistent or Transient Configuration Change in SLAX and XSLT Commit Scripts*
- *Creating a Commit Script Macro to Read the Custom Syntax and Generate Related Configuration Statements*

 Copyright © 2018, Juniper Networks, Inc.

apply-macro

Syntax

```
apply-macro apply-macro-name {
   parameter-name parameter-value;
}
```

Hierarchy Level

All hierarchy levels

Release Information

Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.2 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Use custom syntax in your configuration, which is expanded into standard Junos OS configuration statements during the commit process using the instructions defined in the corresponding commit script macro.

Macros work by locating **apply-macro** statements that you include in the candidate configuration and using the values specified in the **apply-macro** statement as parameters to a set of instructions (the macro) defined in a commit script. The commit script alters your configuration from one that contains custom syntax into a full configuration containing standard Junos OS statements.

In effect, your custom configuration syntax serves a dual purpose. The syntax allows you to simplify your configuration tasks, and it provides data (or *hooks*) that are used by commit script macros.

You can include the **apply-macro** statement at any level of the configuration hierarchy. You can include multiple **apply-macro** statements at each level of the configuration hierarchy; however, each must have a unique name.

Options

apply-macro-name—Name of the **apply-macro** statement.

parameter-name—One or more parameters. Parameters can be any text you want to include in your configuration.

parameter-value—A value that corresponds to the parameter name. Parameter values can be any text you want to include in your configuration.

Required Privilege Level

configure—To enter configuration mode; other required privilege levels depend on where the statement is located in the configuration hierarchy.

Related Documentation

- *Overview of Creating Custom Configuration Syntax with Commit Script Macros*

checksum

Syntax checksum (md5 | sha-256 | sha1) *hash*;

Hierarchy Level [edit event-options event-script file *filename*],
[edit system scripts commit file *filename*],
[edit system scripts op file *filename*],
[edit system scripts snmp file *filename*],
[edit system extensions extension-service application file *filename*]

Release Information Statement introduced in Junos OS Release 9.5.
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.
Statement introduced for the **[edit system extensions extension-service application file *filename*]** hierarchy level in Junos OS Release 16.1 for MX80, MX104, MX240, MX480, MX960, MX2010, MX2020, vMX Series.

Description For Junos OS commit scripts, event scripts, op scripts, SNMP scripts, and scripts developed using the Juniper Extension Toolkit (JET) specify the MD5, SHA-1, or SHA-256 checksum hash. When Junos OS executes a local commit, event, op, or SNMP script, the system verifies the authenticity of the script by using the configured checksum hash.

Options **md5 *hash***—MD5 checksum of this script.

sha-256 *hash*—SHA-256 checksum of this script.

sha1 *hash*—SHA-1 checksum of this script.

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

Related Documentation

- *Configuring Checksum Hashes for a Commit Script*
- *Configuring Checksum Hashes for an Event Script*
- *Configuring Checksum Hashes for an Op Script*
- *Configuring Checksum Hashes for an SNMP Script*
- *Executing an Op Script from a Remote Site*
- *file checksum md5* command in the *System Basics and Services Command Reference*
- *file checksum sha-256* command in the *System Basics and Services Command Reference*
- *file checksum sha1* command in the *System Basics and Services Command Reference*

 Copyright © 2018, Juniper Networks, Inc.

command

Syntax command *filename-alias*;

Hierarchy Level [edit system scripts op file *filename*]

Release Information Statement introduced in Junos OS Release 7.6.
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 a filename alias for an op script file. This allows you to run the op script by referencing either the script filename or the filename alias.

Options ***filename-alias***—Alias for the op script file.

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

Related Documentation

- *Enabling an Op Script and Defining a Script Alias*

commit

Syntax

```
commit {
  allow-transients;
  dampen {
    dampen-options {
      cpu-factor cpu-factor;
      line-interval line-interval;
      time-interval time-interval;
    }
  }
  direct-access;
  file filename {
    checksum (md5 | sha-256 | sha1) hash;
    optional;
    refresh;
    refresh-from url;
    source url;
  }
  max-datasize size;
  refresh;
  refresh-from url;
  traceoptions {
    file <filename> <files number> <size size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
  }
}
```

Hierarchy Level

[edit system scripts]

Release Information

Statement introduced in Junos OS Release 7.4.
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

For Junos OS commit scripts, configure the commit-time scripting mechanism.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Commit Script Overview*
- How Commit Scripts Work on page 52
- *Storing and Enabling Scripts*

Copyright © 2018, Juniper Networks, Inc.

description

Syntax description *description*;

Hierarchy Level [edit system scripts op file *filename*]
[edit system scripts op file *filename* arguments *argument-name*]

Release Information Statement introduced in Junos OS Release 7.6.
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 Provide help text to describe an op script or its command-line arguments. The help text is included in the context-sensitive help in the command-line interface (CLI).

Options ***description***—At the script hierarchy level, specify the purpose of the script. At the arguments hierarchy level, provide a description for the command-line argument.

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

Related Documentation
- *Configuring Help Text for Op Scripts*
- *Declaring and Using Command-Line Arguments in Op Scripts*
- file (Op Scripts) on page 87

direct-access

Syntax direct-access;

Hierarchy Level [edit system scripts commit]

Release Information Statement introduced in Junos OS Release 9.1.
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 that commit scripts read input configurations directly from the database.

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

Related Documentation
- *Executing Large Commit Scripts*

file (Commit Scripts)

Syntax

```
file filename {
   checksum (md5 | sha-256 | sha1) hash;
   optional;
   refresh;
   refresh-from url;
   source url;
}
```

Hierarchy Level

[edit system scripts commit]

Release Information

Statement introduced in Junos OS Release 7.4.
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

Enable a Junos OS commit script that is located in the **/var/db/scripts/commit** directory on the hard disk or the **/config/scripts/commit** directory on the flash drive. During a commit operation, enabled commit scripts are executed in the order specified in the configuration.

Options

filename—Name of a Python, Extensible Stylesheet Language Transformations (XSLT), or Stylesheet Language Alternative syntaX (SLAX) file containing a commit script.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Storing and Enabling Scripts*
- *Controlling Execution of Commit Scripts During Commit Operations*

Copyright © 2018, Juniper Networks, Inc.

file (Op Scripts)

Syntax

```
file filename {
  allow-commands "regular-expression";
  arguments {
    argument-name {
      description descriptive-text;
    }
  }
  checksum (md5 | sha-256 | sha1) hash;
  command filename-alias;
  dampen {
    dampen-options {
      cpu-factor cpu-factor;
      line-interval line-interval;
      time-interval time-interval;
    }
  }
  description descriptive-text;
  refresh;
  refresh-from url;
  source url;
}
```

Hierarchy Level

[edit system scripts op]

Release Information

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Enable a Junos OS op script that is located in the **/var/db/scripts/op** directory on the hard disk or the **/config/scripts/op** directory on the flash drive. After enabling an op script, you can execute the script from the CLI using the **op** command.

Options

filename—Name of a Python, Extensible Stylesheet Language Transformations (XSLT), or Stylesheet Language Alternative syntaX (SLAX) file containing an op script.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Storing and Enabling Scripts*
- *Enabling an Op Script and Defining a Script Alias*

no-allow-url (Op Scripts)

Syntax no-allow-url;

Hierarchy Level [edit system scripts op]

Release Information Statement introduced in Junos OS Release 10.0.
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 Prohibit the remote execution of Junos OS op scripts. When you include this configuration statement, the **op url** operational mode command does not support executing op scripts from a remote site and generates an error.

Default If you do not include the **no-allow-url** statement, authorized users can issue the **op url** command to execute op scripts from a remote site.

NOTE: You must configure the **allow-url-for-python** statement in order to execute Python automation scripts from a remote site.

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

Related Documentation

- file (Op Scripts) on page 87
- *Executing an Op Script from a Remote Site*

 Copyright © 2018, Juniper Networks, Inc.

op

Syntax

```
op {
  allow-url-for-python;
  dampen {
    dampen-options {
      cpu-factor cpu-factor;
      line-interval line-interval;
      time-interval time-interval;
    }
  }
  file filename {
    allow-commands "regular-expression";
    arguments {
      argument-name {
        description descriptive-text;
      }
    }
    checksum (md5 | sha-256 | sha1) hash;
    command filename-alias;
    dampen {
      dampen-options {
        cpu-factor cpu-factor;
        line-interval line-interval;
        time-interval time-interval;
      }
    }
    description descriptive-text;
    refresh;
    refresh-from url;
    source url;
  }
  max-datasize size;
  no-allow-url
  refresh;
  refresh-from url;
  traceoptions {
    file <filename> <files number> <size size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
  }
}
```

Hierarchy Level

[edit system scripts]

Release Information

Statement introduced in Junos OS Release 7.6.
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 an operation scripting mechanism.

Options

The remaining statements are explained separately. See CLI Explorer.

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

Related Documentation
- *Storing and Enabling Scripts*

optional

Syntax
optional;

Hierarchy Level
[edit system scripts commit file *filename*]

Release Information
Statement introduced in Junos OS Release 7.4.
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
Allow a commit operation to succeed even if the commit script specified in the **file** statement is missing from the appropriate commit script directory on the device.

NOTE: Commit scripts are stored on a device's hard disk in the /var/db/scripts/commit directory or on the flash drive in the /config/scripts/commit directory. On the QFabric system, commit scripts are stored in the /pbdata/mgd_shared/*partition-ip*/var/db/scripts/commit/ directory on the Director device.

Default
If you do not include the **optional** statement for a commit script, the commit operation fails if that script is absent from the commit script directory.

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

Related Documentation
- *Controlling Execution of Commit Scripts During Commit Operations*

Copyright © 2018, Juniper Networks, Inc.

refresh (Commit Scripts)

Syntax refresh;

Hierarchy Level [edit system scripts commit],
[edit system scripts commit file *filename*]

Release Information Statement introduced in Junos OS Release 7.4.
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 Overwrite the local copy of all enabled commit scripts or a single enabled commit script with the copy located at the source URL, as specified in the **source** statement at the same hierarchy level. If the **load-scripts-from-flash** statement is configured, the device refreshes the scripts on the flash drive instead of the hard disk.

The update operation occurs as soon as you issue the **set refresh** configuration mode command. Issuing the **set refresh** command does not add the **refresh** statement to the configuration. Thus the command behaves like an operational mode command by executing an operation, instead of adding a statement to the configuration.

NOTE: On the QFabric system, commit scripts are stored in the /pbdata/mgd_shared/*partition-ip*/var/db/scripts/commit/ directory on the Director device.

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

Related Documentation

- *Configuring and Using a Master Source Location for a Script*
- *Example: Configuring and Refreshing from the Master Source for a Script*
- refresh-from (Commit Scripts) on page 93
- source (Commit Scripts) on page 97

refresh (Op Scripts)

Syntax

refresh;

Hierarchy Level

[edit system scripts op],
[edit system scripts op file *filename*]

Release Information

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 11.1 on the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Overwrite the local copy of all enabled op scripts or a single enabled op script with the copy located at the source URL, as specified in the **source** statement at the same hierarchy level. If the **load-scripts-from-flash** statement is configured, the device refreshes the scripts on the flash drive instead of the hard disk.

The update operation occurs as soon as you issue the **set refresh** configuration mode command. Issuing the **set refresh** command does not add the **refresh** statement to the configuration. Thus the command behaves like an operational mode command by executing an operation, instead of adding a statement to the configuration.

NOTE: On the QFabric system, op scripts are stored in the /pbdata/mgd_shared/*partition-ip*/var/db/scripts/op/ directory on the Director device.

Required Privilege Level

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

Related Documentation

- *Configuring and Using a Master Source Location for a Script*
- *Example: Configuring and Refreshing from the Master Source for a Script*
- refresh-from (Op Scripts) on page 94
- source (Op Scripts) on page 98

Copyright © 2018, Juniper Networks, Inc.

refresh-from (Commit Scripts)

Syntax

refresh-from *url*;

Hierarchy Level

[edit system scripts commit],
[edit system scripts commit file *filename*]

Release Information

Statement introduced in Junos OS Release 7.4.
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

Overwrite the local copy of all enabled commit scripts or a single enabled commit script with the copy located at the specified URL. If the **load-scripts-from-flash** statement is configured, the device refreshes the scripts on the flash drive instead of the hard disk.

The update operation occurs as soon as you issue the **set refresh-from *url*** configuration mode command. Issuing the **set refresh-from** command does not add the **refresh-from** statement to the configuration. Thus the command behaves like an operational mode command by executing an operation, instead of adding a statement to the configuration.

NOTE: **This statement is not supported on the QFabric system.**

Options

url—The source specified as a Hypertext Transfer Protocol (HTTP) URL, FTP URL, or secure copy (scp)-style remote file specification.

Required Privilege Level

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

Related Documentation

- *Using an Alternate Source Location for a Script*
- refresh (Commit Scripts) on page 91
- source (Commit Scripts) on page 97

refresh-from (Op Scripts)

Syntax

refresh-from *url*;

Hierarchy Level

[edit system scripts op],
[edit system scripts op file *filename*]

Release Information

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 11.1 on the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Overwrite the local copy of all enabled op scripts or a single enabled op script with the copy located at the specified URL. If the **load-scripts-from-flash** statement is configured, the device refreshes the scripts on the flash drive instead of the hard disk.

The update operation occurs as soon as you issue the **set refresh-from *url*** configuration mode command. Issuing the **set refresh-from** command does not add the **refresh-from** statement to the configuration. Thus the command behaves like an operational mode command by executing an operation, instead of adding a statement to the configuration.

NOTE: **This statement is not supported on the QFabric system.**

Options

url—Source specified as a Hypertext Transfer Protocol (HTTP) URL, FTP URL, or secure copy (scp)-style remote file specification.

Required Privilege Level

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

Related Documentation

- *Using an Alternate Source Location for a Script*
- refresh (Op Scripts) on page 92
- source (Op Scripts) on page 98

Copyright © 2018, Juniper Networks, Inc.

scripts

Syntax

```
scripts {
  commit {
    allow-transients;
    dampen {
      dampen-options {
        cpu-factor cpu-factor;
        line-interval line-interval;
        time-interval time-interval;
      }
    }
    direct-access;
    file filename {
      checksum (md5 | sha-256 | sha1) hash;
      optional;
      refresh;
      refresh-from url;
      source url;
    }
    max-datasize size;
    refresh;
    refresh-from url;
    traceoptions {
      file <filename> <files number> <size size> <world-readable | no-world-readable>;
      flag flag;
      no-remote-trace;
    }
  }
  language python;
  load-scripts-from-flash;
  op {
    allow-url-for-python;
    dampen {
      dampen-options {
        cpu-factor cpu-factor;
        line-interval line-interval;
        time-interval time-interval;
      }
    }
    file filename {
      allow-commands "regular-expression";
      arguments {
        argument-name {
          description descriptive-text;
        }
      }
      checksum (md5 | sha-256 | sha1) hash;
      command filename-alias;
      dampen {
        dampen-options {
          cpu-factor cpu-factor;
          line-interval line-interval;
          time-interval time-interval;
```

```
            }
          }
          description descriptive-text;
          refresh;
          refresh-from url;
          source url;
        }
        max-datasize size;
        no-allow-url
        refresh;
        refresh-from url;
        traceoptions {
          file <filename> <files number> <size size> <world-readable | no-world-readable>;
          flag flag;
          no-remote-trace;
        }
      }
      snmp {
        file filename {
          checksum (md5 | sha-256 | sha1) hash;
          oid id {
            priority;
          }
          python-script-user username;
          refresh;
          refresh-from;
          source;
        }
        max-datasize size;
        refresh;
        refresh-from;
        traceoptions {
          file <filename> <files number> <size size> <world-readable | no-world-readable>;
          flag flag;
          no-remote-trace;
        }
      }
      synchronize;
    }
```

Hierarchy Level [edit system]

Release Information Statement introduced in Junos OS Release 7.4.
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 scripting mechanisms for Junos OS commit, op, or SNMP scripts.

NOTE: The **traceoptions** statement is not supported on QFabric systems.

Copyright © 2018, Juniper Networks, Inc.

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

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

Related Documentation
- *Commit Script Overview*
- *Op Script Overview*
- *Storing and Enabling Scripts*

source (Commit Scripts)

Syntax source *url*;

Hierarchy Level [edit system scripts commit file *filename*]

Release Information
Statement introduced in Junos OS Release 7.4.
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 the location of the master source file for a commit script. When you issue the **set refresh** configuration mode command at the same hierarchy level, the local copy of the script is overwritten by the version stored at the specified URL. If the **load-scripts-from-flash** statement is configured, the device refreshes the scripts on the flash drive instead of the hard disk.

NOTE: On the QFabric system, commit scripts are stored in the **/pbdata/mgd_shared/*partition-ip*/var/db/scripts/op/** directory on the Director device.

Options ***url***—The source specified as an HTTP URL, FTP URL, or scp-style remote file specification.

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

Related Documentation
- *Configuring and Using a Master Source Location for a Script*
- *Example: Configuring and Refreshing from the Master Source for a Script*
- *Overview of Updating Scripts from a Remote Source*
- refresh (Commit Scripts) on page 91
- refresh-from (Commit Scripts) on page 93

source (Op Scripts)

Syntax source *url*;

Hierarchy Level [edit system scripts op file *filename*]

Release Information Statement introduced in Junos OS Release 7.6.
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 the location of the master source file for an op script. When you issue the **set refresh** configuration mode command at the same hierarchy level, the local copy of the script is overwritten by the version stored at the specified URL. If the **load-scripts-from-flash** statement is configured, the device refreshes the scripts on the flash drive instead of the hard disk.

NOTE: On the QFabric system, commit scripts are stored in the /pbdata/mgd_shared/*partition-ip*/var/db/scripts/op/ directory on the Director device.

Options ***url***—Master source file for an op script specified as an HTTP URL, FTP URL, or scp-style remote file specification.

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

Related Documentation

- *Configuring and Using a Master Source Location for a Script*
- *Example: Configuring and Refreshing from the Master Source for a Script*
- refresh (Op Scripts) on page 92
- refresh-from (Op Scripts) on page 94

 Copyright © 2018, Juniper Networks, Inc.

CHAPTER 6

Junos Space

- Understanding Junos Space Support on page 99

Understanding Junos Space Support

The Juniper Networks Junos Space application, running on a JA1500 appliance or a Junos Space Virtual Appliance, is a comprehensive platform for building and deploying applications for collaboration, productivity, and network infrastructure and operations management. Junos Space provides a runtime environment implemented as a fabric of virtual and physical appliances.

The Junos Space Network Management Platform software comprises various applications for network management and configuration, including:

- Junos Space Administration—Provides management of Junos Space fabric, databases, licenses, applications, authentication servers, tags, permission labels, DMI schemas, and troubleshooting.
- Network Director—Provides unified management of supported Juniper Networks devices in your network. By providing full network life cycle management, Network Director simplifies the discovery, configuration, visualization, monitoring, and administration of large networks.
- Service Automation—Provides an end-to-end solution designed to streamline operations and enable proactive network management for Junos OS devices. The solution consists of Advanced Insight Scripts (AI-Scripts), Junos Space Service Now and Service Insight applications, and Juniper Support Systems (JSS).

NOTE: **Do not install Junos Space and AI-Scripts on the control plane network EX4200 switches or EX4200 Virtual Chassis in a QFX3000 QFabric system**

Before you can use Junos Space Network Director to manage the QFX Series device, you must ensure that the configuration on the device meets the requirements for all managed devices. For example:

- The device configuration has a static management IP address that is reachable from the Junos Space server.
- There is a user with full administrative privileges for Junos Space administration.
- SNMP is enabled (only if you plan on using SNMP as part of the device discovery).
- In Junos Space, set up a default device management interface (DMI) schema for the QFX Series device.

For more information about Network Director requirements, see the *Network Director Quick Start Guide* at:

https://www.juniper.net/documentation/en_US/network-director1.5/information-products/pathway-pages/index.html

For more information about Junos Space, go to:

https://www.juniper.net/documentation/en_US/release-independent/junos-space/index.html

Related Documentation

- Configuring SNMP on page 254
- Configuring SSH Service for Remote Access to the Router or Switch on page 9

Copyright © 2018, Juniper Networks, Inc.

PART 3

Network Analytics

- Configuring Network Analytics on page 103
- Network Analytics Configuration Statements on page 137
- Network Analytics Operational Commands on page 155

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 7

Configuring Network Analytics

- Network Analytics Overview on page 103
- Understanding Network Analytics Configuration and Status on page 111
- Understanding Network Analytics Streaming Data on page 112
- Understanding Enhanced Network Analytics Streaming Data on page 115
- Understanding Enhanced Analytics Local File Output on page 120
- Prototype File for the Google Protocol Buffer Stream Format on page 122
- Configuring Queue Monitoring on page 123
- Configuring Traffic Monitoring on page 125
- Configuring a Local File for Network Analytics Data on page 126
- Configuring a Remote Collector for Streaming Analytics Data on page 127
- Example: Configuring Network Analytics on page 129

Network Analytics Overview

The network analytics feature provides visibility into the performance and behavior of the data center infrastructure. This feature collects data from the switch, analyzes the data using sophisticated algorithms, and captures the results in reports. Network administrators can use the reports to help troubleshoot problems, make decisions, and adjust resources as needed. The analytics manager (analyticsm) in the Packet Forwarding Engine collects traffic and queue statistics, and the analytics daemon (analyticsd) in the Routing Engine analyzes the data and generates reports. You can enable network analytics by configuring microburst monitoring and high-frequency traffic statistics monitoring.

NOTE: In Junos OS Release 13.2X51-D15, the network analytics feature was enhanced, and extensive changes were made to the CLI statements and hierarchies. If you upgrade to Junos OS Release 13.2X51-D15 or later from a release prior to 13.2X51-D15, network analytics configurations committed in previous releases will appear on your device, but the feature is disabled. To enable this feature, you must reconfigure it using the new CLI statements and hierarchies.

For more information, see:

- Analytics Feature Overview on page 104
- Network Analytics Enhancements Overview on page 105
- Summary of CLI Changes on page 106

Analytics Feature Overview

You enable network analytics by configuring queue (microburst) monitoring and high-frequency traffic statistics monitoring.You use microburst monitoring to look at traffic queue conditions in the network. A microburst occurrence indicates to the Packet Forwarding Engine that a user-specified queue depth or latency threshold is reached. The queue depth is the buffer (in bytes) containing the data, and latency is the time (in nanoseconds or microseconds) the data stays in the queue.

You can configure queue monitoring based on either queue depth or latency (but not both), and configure the frequency (polling interval) at which the Packet Forwarding Engine checks for microbursts and sends the data to the Routing Engine for processing. You may configure queue monitoring globally for all physical interfaces on the system, or for a specific interface on the switch. However, the specified queue monitoring interval applies either to all interfaces, or none; you cannot configure the interval for each interface.

You use high-frequency traffic statistics monitoring to collect traffic statistics at specified polling intervals. Similar to the queue monitoring interval, the traffic monitoring interval applies either to all interfaces, or none; you cannot configure the interval for each interface.

Both traffic and queue monitoring are disabled by default. You must configure each type of monitoring using the CLI. In each case, the configuration for an interface always takes precedence over the global configuration.

NOTE: **You can configure traffic and queue monitoring for physical interfaces only; logical interfaces and Virtual Chassis port (VCP) interfaces are not supported.**

The analyticsd daemon in the Routing Engine generates local log files containing queue and traffic statistics records. You can specify the log filename and size, and the number of log files. If you do not configure a filename, the data is not saved.

You can display the local log file or specify a server to receive the streaming data containing the queue and traffic statistics.

For each port, information for the last 10 records of traffic statistics and 100 records of queue statistics is cached. You may view this information by using the **show analytics** commands.

To store traceoptions data, you configure the **traceoptions** statement at the **[edit services analytics]** hierarchy level.

Copyright © 2018, Juniper Networks, Inc.

Network Analytics Enhancements Overview

Beginning in Junos OS Release 13.2X51-D15, the network analytics feature provides the following enhancements:

- Resources—Consist of interfaces and system. The interfaces resource allows you to configure an interface name and an associated resource profile name for each interface. With the system resource, you can configure the polling intervals for queue monitoring and traffic monitoring, and an associated resource profile for the system.
- Resource profile—A template that contains the configurations for queue and traffic monitoring, such as depth threshold and latency threshold values, and whether each type of monitoring is enabled or disabled. Once a resource profile is configured, you apply it to a system or interfaces resource.
- Collector—A server for collecting queue and traffic monitoring statistics, and can be a local or remote server. You can configure a local server to store monitoring statistics in a log file, or a remote server to receive streamed statistics data.
- Export profile—You must configure an export profile if you wish to send streaming data to a remote collector. In the export profile, you define the category of streamed data (system-wide or interface-specific) to determine stream type the collector will receive. You can specify both system and interface stream categories. System data includes system information and status of queue and traffic monitoring. Interface-specific data includes interface information, queue and traffic statistics, and link, queue, and traffic status.
- Google Protocol Buffer (GBP) stream format—A new streaming format for monitoring statistics data that is sent to a remote collector in a single AnRecord message. This stream format provides nine types of information, including:
  - System information—General system information, including boot time, model information, serial number, number of ports, and so on.
  - System queue status—Queue status for the system in general.
  - System traffic status—Traffic status for the system in general.
  - Interface information—Includes SNMP index, slot, port, and other information.
  - Queue statistics for interfaces—Queue statistics for specific interfaces.
  - Traffic statistics for interfaces—Traffic statistics for specific interfaces.
  - Link status for interfaces—Includes link speed, state, and so on.
  - Queue status for interfaces—Queue status for specific interfaces.
  - Traffic status for interfaces—Traffic status for specific interfaces.
- The **analytics.proto** file—Provides a template for the GBP stream format. This file can be used for writing your analytics server application. To download the file, go to:

  https://www.juniper.net/documentation/en_US/junos13.2/topics/reference/proto-files/analytics-proto.txt
- Use of threshold values—The Analytics Manager (analyticsm) will generate a queue statistics record when the lower queue depth or latency threshold value is exceeded.

- User Datagram Protocol (UDP)—Additional transport protocol you can configure, in addition to Transmission Control Protocol (TCP), for the remote streaming server port.
- Single file for local logging—Replaces the separate log files for queue and traffic statistics.
- Change in latency measurement—Configuration and reporting of latency values have changed from microseconds to nanoseconds.
- Change in reporting of the collection time in UTC format—Statistics collection time is reported in microseconds instead of milliseconds.
- New operational mode command **show analytics collector**—Replaces the **show analytics streaming-server** command.
- Changes in command output format—Include the following changes:
  - Addition of unicast, multicast, and broadcast packet counters in queue and traffic statistics.
  - Reversal of the sequence of statistics information in the output. The most recent record is displayed at the beginning, and the oldest record at the end of the output.
  - Removal of traffic or queue monitoring status information from the global portion of the **show analytics configuration** and **show analytics status** command output if there is no global configuration.
  - Addition of **n/a** to the interface-specific portion of the **show analytics configuration** and **show analytics status** command output if a parameter is not configured (for example, depth threshold or latency threshold).

Summary of CLI Changes

Beginning in Junos OS Release 13.2X51-D15, enhancements to the network analytics feature result in changes in the CLI when you configure the feature. See Table 11 on page 106 for a summary of CLI changes.

Table 11: Network Analytics CLI Changes

Task	CLI for Junos OS Release 13.2X50-D15 and 13.2X51-D10	CLI for Junos OS Release 13.2X51-D15 and later

Configuring global queue and traffic monitoring polling interval	**[edit services analytics]**
	traffic-statistics {
	interval *interval*;
	}
	queue-statistics {
	interval *interval*;
	}
		[edit services analytics]
		resource {
		system {
		polling-interval {
		queue-monitoring *interval*;
		traffic-monitoring *interval*;
		}
		}
		}

Copyright © 2018, Juniper Networks, Inc.

Table 11: Network Analytics CLI Changes *(continued)*

Task	CLI for Junos OS Release 13.2X50-D15 and 13.2X51-D10	CLI for Junos OS Release 13.2X51-D15 and later

Configuring local files for traffic and queue statistics reporting	**[edit services analytics]**
	
	traffic-statistics {
	file *filename*;
	size *size*;
	files *number*;
	}
	queue-statistics {
	file *filename*;
	size *size*;
	files *number*;
	}
		[edit services analytics]
		
		collector {
		local {
		file *filename* {
		files *number*;
		size *size*;
		}
		}
		}

Enabling queue statistics and traffic monitoring, and specifying the depth threshold for all interfaces (globally)	**[edit services analytics]**
	
	interfaces {
	all {
	queue-statistics;
	traffic-statistics;
	depth-threshold {
	high *number*;
	low *number*;
	}
	}
	}
		Requires defining a resource profile and applying it to the system:
		
		1. To define a resource profile:
		
		[edit services analytics]
		
		resource-profiles {
		profile-name{
		queue-monitoring;
		traffic-monitoring;
		depth-threshold {
		high *number*;
		low *number*;
		}
		}
		}
		
		2. To apply a profile to the system:
		
		[edit services analytics]
		
		resource {
		system {
		resource-profile *profile-name*;
		}
		}

Table 11: Network Analytics CLI Changes *(continued)*

Task	CLI for Junos OS Release 13.2X50-D15 and 13.2X51-D10	CLI for Junos OS Release 13.2X51-D15 and later

Enabling queue statistics and traffic monitoring, and specifying the latency threshold for one interface	**[edit services analytics]**
	
	interfaces {
	interface{
	queue-statistics;
	traffic-statistics;
	latency-threshold
	high *number*;
	low *number*;
	}
	}
		Requires defining a resource profile and applying it to the interface:
		
		1. To define a resource profile:
		
		[edit services analytics]
		
		resource-profiles {
		profile-name{
		queue-monitoring;
		traffic-monitoring;
		latency-threshold {
		high *number*;
		low *number*;
		}
		}
		}
		
		2. To apply a profile to the interface:
		
		[edit services analytics]
		
		resource {
		interfaces {
		interface-name {
		resource-profile *profile-name*;
		}
		}
		}

Configuring the streaming data format (JSON, CSV, or TSV) to send to a remote server
 	
NOTE: Junos OS Release 13.2X51-D15 added support for the GPB stream format and configuration of the transport protocols (TCP or UDP).
	[edit services analytics]
	
	streaming-servers {
	address *ip-address* {
	port *number* {
	stream-format *format*;
	}
	}
	}
		Requires defining the stream format in an export profile and applying the profile to the collector.
		
		1. To configure the stream format:
		
		[edit services analytics]
		
		export-profiles {
		profile-name {
		stream-format *format*;
		}
		}
		
		2. To apply an export profile to the collector:
		
		[edit services analytics]
		
		collector {
		address *ip-address* {
		port *number* {
		transport *protocol* {
		export-profile *profile-name*;
		}
		}
		}
		}

Copyright © 2018, Juniper Networks, Inc.

Table 11: Network Analytics CLI Changes *(continued)*

Task	CLI for Junos OS Release 13.2X50-D15 and 13.2X51-D10	CLI for Junos OS Release 13.2X51-D15 and later

Configuring the streaming message types (queue or traffic statistics) to send to a remote server	**[edit services analytics]**
	
	streaming-servers {
	address *ip-address* {
	port *number* {
	stream-type *type*;
	stream-type *type*;
	}
	}
	}
		Requires defining an export profile and applying it to the collector:
		
		1. To define an export profile:
		
		[edit services analytics]
		
		export-profiles {
		profile-name {
		interface {
		information;
		statistics {
		queue;
		traffic;
		}
		status {
		link;
		queue;
		traffic;
		}
		}
		system {
		information;
		status {
		queue;
		traffic;
		}
		}
		}
		}
		
		2. To apply an export profile to the collector:
		
		[edit services analytics]
		
		collector {
		address *ip-address* {
		port *number* {
		export-profile *profile-name*;
		}
		}
		}

Table 11: Network Analytics CLI Changes *(continued)*

Task	CLI for Junos OS Release 13.2X50-D15 and 13.2X51-D10	CLI for Junos OS Release 13.2X51-D15 and later

Configuring the transport protocol for sending streaming data to an external server	No configuration is available. Only the TCP protocol is supported.	Configuration is available. Both TCP and UDP protocols are supported, and can be configured for the same port.
		
		[edit services analytics]
		
		collector {
		address *ip-address* {
		port *number1* {
		transport tcp;
		transport udp;
		}
		port *number2* {
		transport udp;
		}
		}
		}

Show information about remote streaming server or collector	Issue the **show analytics streaming-sever** command.	Issue the **show analytics collector** command.

Release History Table

Release	Description
13.2X51-D15	In Junos OS Release 13.2X51-D15, the network analytics feature was enhanced, and extensive changes were made to the CLI statements and hierarchies.
13.2X51-D15	Beginning in Junos OS Release 13.2X51-D15, the network analytics feature provides the following enhancements:
13.2X51-D15	Beginning in Junos OS Release 13.2X51-D15, enhancements to the network analytics feature result in changes in the CLI when you configure the feature.

Related Documentation

- analytics on page 138

Copyright © 2018, Juniper Networks, Inc.

Understanding Network Analytics Configuration and Status

The network analytics feature provides visibility into the performance and behavior of the data center infrastructure. You can enable network analytics by configuring traffic and queue statistics monitoring.

NOTE: **This topic describes the configuration and status output from Junos OS Release 13.2X50-D15 and 13.2X51-D10 only.**

If you had enabled traffic or queue monitoring, you can issue the **show analytics configuration** and **show analytics status** commands to view the global interface configuration and status and that of specific interfaces. The output that is displayed depends on your configuration at the global interface and specific interface levels. For example:

- A global interface configuration (for all interfaces) to disable monitoring supersedes the configuration to enable it on an interface.
- The interface configuration to enable or disable monitoring supersedes the global interface configuration, unless monitoring had been disabled globally for all interfaces.
- If there is no configuration, whether for all interfaces or a specific interface, monitoring is disabled by default (see Table 12 on page 111).

Table 12 on page 111 describes the correlation between the user configuration and the settings that are displayed.

Table 12: Configuration and Status Output in Junos OS Release 13.2X51-D10 and 13.2X50-D15

User Configuration	Global or System Settings		Specific Interface Settings	
	Configuration	Status	Configuration	Status
No global or specific interface configuration. This is the default setting.	Auto	Auto	Auto	Disabled
No global interface configuration but the specific interface monitoring is disabled.	Auto	Auto	Disabled	Disabled
No global interface configuration but the specific interface monitoring is enabled.	Auto	Auto	Enabled	Enabled
Monitoring is disabled globally and there is no interface configuration.	Disabled	Disabled	Auto	Disabled
Monitoring is disabled at both the global and specific interface levels.	Disabled	Disabled	Disabled	Disabled

Copyright © 2018, Juniper Networks, Inc.

Table 12: Configuration and Status Output in Junos OS Release 13.2X51-D10 and 13.2X50-D15 *(continued)*

User Configuration	Global or System Settings		Specific Interface Settings	
	Configuration	Status	Configuration	Status
Monitoring is disabled at the global interface level but is enabled at the specific interface level. The global interface *Disabled* setting supersedes the *Enabled* setting for a specific interface.	Disabled	Disabled	Enabled	Disabled
Monitoring is enabled for all interfaces but there is no configuration for the specific interface .	Enabled	Enabled	Auto	Enabled
Monitoring is enabled at both the global and specific interface levels.	Enabled	Enabled	Enabled	Enabled
Monitoring is enabled for all interfaces but is disabled for the specific interface.	Enabled	Enabled	Disabled	Disabled

Related Documentation

- Network Analytics Overview on page 103
- analytics on page 138
- queue-statistics on page 148
- traffic-statistics on page 153
- show analytics configuration on page 161
- show analytics status on page 167

Understanding Network Analytics Streaming Data

This topic describes the network analytics queue and traffic statistics that are streamed to remote servers.

You can configure one or more remote servers to receive streamed data containing queue and traffic statistics. The format of the streamed data can be Javascript Object Notation (JSON), Comma-separated Values (CSV), or Tab-separated Values (TSV).

NOTE: **The output shown in this topic applies to Junos OS Release 13.2X51-D10 only. The time is displayed in the Unix epoch format (also known as Unix time or POSIX time).**

The following examples show the streamed queue statistics data output in different formats.

- JSON format:

Copyright © 2018, Juniper Networks, Inc.

```
{"record-type":"queue-stats","time":1383453988263,"router-id":"qfx5100-switch",
"port":"xe-0/0/18","latency":0,"queue-depth":208}
```

- CSV format:

```
q,1383454067604,qfx5100-switch,xe-0/0/18,0,208
```

- TSV format:

```
q       585870192561703872      qfx5100-switch       xe-0/0/18       (null)
208     2
```

Table 13 on page 113 describes the output fields for streamed queue statistics data in the order they appear.

Table 13: Streamed Queue Statistics Data Output Fields

Field	Description
record-type	Type of statistics. Displayed as: • **queue-stats** (JSON format) • **q** (CSV or TSV format)
time	Time (in Unix epoch format) at which the statistics were captured.
router-id	ID of the network analytics host device.
port	Name of the physical port configured for network analytics.
latency	Traffic queue latency in milliseconds.
queue depth	Depth of the traffic queue in bytes.

The following examples show the streamed traffic statistics data output in different formats.

- JSON format:

```
{"record-type":"traffic-stats","time":1383453986763,"router-id":"qfx5100-switch",
"port":"xe-0/0/16","rxpkt":26524223621,"rxpps":8399588,"rxbyte":3395100629632,
"rxbps":423997832,"rxdrop":0,"rxerr":0,"txpkt":795746503,"txpps":0,"txbyte":101855533467,
"txbps":0,"txdrop":0,"txerr":0}
```

- CSV format:

```
t,1383454072924,qfx5100-switch,xe-0/0/19,1274299748,82950,163110341556,85603312,0,0,
27254178291,8300088,3488534810679,600002408,27268587050,3490379142400
```

- TSV format:

```
t       1383454139025   qfx5100-switch  xe-0/0/19       1279874033      82022
163823850036    84801488        0       0       27811618258     8199630
3559887126455   919998736       27827356915     3561901685120
```

Table 14 on page 114 describes the output fields for streamed traffic statistics data in the order they appear.

Table 14: Streamed Traffic Statistics Data Output Fields

Field	Description
record-type	Type of statistics. Displayed as: • **traffic-stats** (JSON format) • **t** (CSV or TSV format)
time	Time (in Unix epoch format) at which the statistics were captured.
router-id	ID of the network analytics host device.
port	Name of the physical port configured for network analytics.
rxpkt	Total packets received.
rxpps	Total packets received per second.
rxbyte	Total bytes received.
rxbps	Total bits received per second.
rxdrop	Total incoming packets dropped.
rxerr	Total packets with errors.
txpkt	Total packets transmitted.
txpps	Total packets transmitted per second.
txbyte	Total bytes transmitted.
txbps	Total bytes transmitted per second.
txdrop	Total transmitted bytes dropped.
txerr	Total transmitted packets with errors (dropped).

Related Documentation

- Network Analytics Overview on page 103
- show analytics streaming-servers on page 171
- streaming-servers on page 150

Copyright © 2018, Juniper Networks, Inc.

Understanding Enhanced Network Analytics Streaming Data

Network analytics monitoring data can be streamed to remote servers called collectors. You can configure one or more collectors to receive streamed data containing queue and traffic statistics. This topic describes the streamed data output.

NOTE: **This topic applies to Junos OS Release 13.2X51-D15 or later.**

Starting in Junos OS Release 13.2X51-D15, network analytics supports the following streaming data formats and output:

- Google Protocol Buffer (GPB) on page 115
- JavaScript Object Notation (JSON) on page 117
- Comma-separated Values (CSV) on page 118
- Tab-separated Values (TSV) on page 118
- Queue Statistics Output for JSON, CSV, and TSV on page 118
- Traffic Statistics Output for JSON, CSV, and TSV on page 119

Google Protocol Buffer (GPB)

Support for the Google Protocol Buffer (GPB) streaming format has been added in Junos OS Release 13.2X51-D15. This streaming format provides:

- Support for nine types of messages, based on resource type (system-wide or interface-specific).
- Sends messages in a hierarchical format.
- You can generate other stream format messages (JSON, CSV, TSV) from GPB formatted messages.
- Includes a 8-byte message header. See Table 15 on page 115 for more information.

Table 15 on page 115 describes the GPB stream format message header.

Table 15: GPB Stream Format Message Header Information

Byte Position	Field
0 to 3	Length of message
4	Message version
5 to 7	Reserved for future use

The following GPB prototype file (**analytics.proto**) provides details about the streamed data:

```
package analytics;

// Traffic statistics related info
message TrafficStatus {
    optional uint32             status          = 1;
    optional uint32             poll_interval   = 2;
}

// Queue statistics related info
message QueueStatus {
    optional uint32             status          = 1;
    optional uint32             poll_interval   = 2;
    optional uint64             lt_high         = 3;
    optional uint64             lt_low          = 4;
    optional uint64             dt_high         = 5;
    optional uint64             dt_low          = 6;
}

message LinkStatus {
    optional uint64             speed           = 1;
    optional uint32             duplex          = 2;
    optional uint32             mtu             = 3;
    optional bool               state           = 4;
    optional bool               auto_negotiation= 5;
}

message InterfaceInfo {
    optional uint32             snmp_index      = 1;
    optional uint32             index           = 2;
    optional uint32             slot            = 3;
    optional uint32             port            = 4;
    optional uint32             media_type      = 5;
    optional uint32             capability      = 6;
    optional uint32             porttype        = 7;
}

message InterfaceStatus {
    optional LinkStatus         link            = 1;
    optional QueueStatus        queue_status    = 2;
    optional TrafficStatus      traffic_status  = 3;
}

message QueueStats {
    optional uint64             timestamp       = 1;
    optional uint64             queue_depth     = 2;
    optional uint64             latency         = 3;
}

message TrafficStats {
    optional uint64             timestamp       = 1;
    optional uint64             rxpkt           = 2;
    optional uint64             rxucpkt         = 3;
    optional uint64             rxmcpkt         = 4;
    optional uint64             rxbcpkt         = 5;
    optional uint64             rxpps           = 6;
    optional uint64             rxbyte          = 7;
    optional uint64             rxbps           = 8;
    optional uint64             rxcrcerr        = 9;
```


Copyright © 2018, Juniper Networks, Inc.

```
    optional uint64             rxdroppkt       = 10;
    optional uint64             txpkt           = 11;
    optional uint64             txucpkt         = 12;
    optional uint64             txmcpkt         = 13;
    optional uint64             txbcpkt         = 14;
    optional uint64             txpps           = 15;
    optional uint64             txbyte          = 16;
    optional uint64             txbps           = 17;
    optional uint64             txcrcerr        = 18;
    optional uint64             txdroppkt       = 19;
}

message InterfaceStats {
    optional TrafficStats       traffic_stats   = 1;
    optional QueueStats         queue_stats     = 2;
}

//Interface message
message Interface {
    required string             name            = 1;
    optional bool               deleted         = 2;
    optional InterfaceInfo      information     = 3;
    optional InterfaceStats     stats           = 4;
    optional InterfaceStatus    status          = 5;
}

message SystemInfo {
    optional uint64             boot_time       = 1;
    optional string             model_info      = 2;
    optional string             serial_no       = 3;
    optional uint32             max_ports       = 4;
    optional string             collector       = 5;
    repeated string             interface_list  = 6;
}

message SystemStatus {
    optional QueueStatus        queue_status    = 1;
    optional TrafficStatus      traffic_status  = 2;
}

//System message
message System {
    required string             name            = 1;
    optional bool               deleted         = 2;
    optional SystemInfo         information     = 3;
    optional SystemStatus       status          = 4;
}

message AnRecord {
    optional uint64             timestamp       = 1;
    optional System             system          = 2;
    repeated Interface          interface       = 3;
}
```

JavaScript Object Notation (JSON)

The JavaScript Object Notation (JSON) streaming format supports the following data:

- Queue statistics data. For example:

```
{"record-type":"queue-stats","time":1383453988263,"router-id":"qfx5100-switch",
"port":"xe-0/0/18","latency":0,"queue-depth":208}
```

See Table 13 on page 113 for more information about queue statistics output fields.

- Traffic statistics. For example:

```
{"record-type":"traffic-stats","time":1383453986763,"router-id":"qfx5100-switch",
"port":"xe-0/0/16","rxpkt":26524223621,"rxpps":8399588,"rxbyte":3395100629632,
"rxbps":423997832,"rxdrop":0,"rxerr":0,"txpkt":795746503,"txpps":0,"txbyte":101855533467,
"txbps":0,"txdrop":0,"txerr":0}
```

See Table 14 on page 114 for more information about traffic statistics output fields.

Comma-separated Values (CSV)

The Comma-separated Values (CSV) streaming format supports the following data:

- Queue statistics. For example:

```
q,1383454067604,qfx5100-switch,xe-0/0/18,0,208
```

See Table 13 on page 113 for more information about queue statistics output fields.

- Traffic statistics. For example:

```
t,1383454072924,qfx5100-switch,xe-0/0/19,1274299748,82950,163110341556,85603312,0,0,
27254178291,8300088,3488534810679,600002408,27268587050,3490379142400
```

See Table 14 on page 114 for more information about traffic statistics output fields.

Tab-separated Values (TSV)

The Tab-separated Values (TSV) streaming format supports the following data:

- Queue statistics. For example:

```
q       585870192561703872      qfx5100-switch       xe-0/0/18       (null)
208     2
```

See Table 13 on page 113 for more information about queue statistics output fields.

- Traffic statistics. For example:

```
t       1383454139025   qfx5100-switch  xe-0/0/19       1279874033      82022
163823850036    84801488        0       0       27811618258     8199630
3559887126455   919998736       27827356915     3561901685120
```

See Table 14 on page 114 for more information about traffic statistics output fields.

Queue Statistics Output for JSON, CSV, and TSV

Table 13 on page 113 describes the output fields for streamed queue statistics data in the order they appear.

Copyright © 2018, Juniper Networks, Inc.

Table 16: Streamed Queue Statistics Data Output Fields

Field	Description
record-type	Type of statistics. Displayed as: • **queue-stats** (JSON format) • **q** (CSV or TSV format)
time	Time (in Unix epoch format) at which the statistics were captured.
router-id	ID of the network analytics host device.
port	Name of the physical port configured for network analytics.
latency	Traffic queue latency in milliseconds.
queue depth	Depth of the traffic queue in bytes.

Traffic Statistics Output for JSON, CSV, and TSV

Table 14 on page 114 describes the output fields for streamed traffic statistics data in the order they appear.

Table 17: Streamed Traffic Statistics Data Output Fields

Field	Description
record-type	Type of statistics. Displayed as: • **traffic-stats** (JSON format) • **t** (CSV or TSV format)
time	Time (in Unix epoch format) at which the statistics were captured.
router-id	ID of the network analytics host device.
port	Name of the physical port configured for network analytics.
rxpkt	Total packets received.
rxpps	Total packets received per second.
rxbyte	Total bytes received.
rxbps	Total bytes received per second.
rxdrop	Total incoming packets dropped.
rxerr	Total packets with errors.
txpkt	Total packets transmitted.

Copyright © 2018, Juniper Networks, Inc.

Table 17: Streamed Traffic Statistics Data Output Fields *(continued)*

Field	Description
txpps	Total packets transmitted per second.
txbyte	Total bytes transmitted.
txbps	Total bytes transmitted per second.
txdrop	Total transmitted bytes dropped.
txerr	Total transmitted packets with errors (dropped).

Release History Table

Release	Description
13.2X51-D15	Starting in Junos OS Release 13.2X51-D15, network analytics supports the following streaming data formats and output:

Related Documentation

- Network Analytics Overview on page 103
- Prototype File for the Google Protocol Buffer Stream Format on page 122
- *address (Analytics Collector)*
- *collector (Analytics)*
- **show analytics collector on page 159**

Understanding Enhanced Analytics Local File Output

The network analytics feature provides visibility into the performance and behavior of the data center infrastructure. You enable network analytics by configuring queue or traffic statistics monitoring, or both. In addition, you can configure a local file for storing the traffic and queue statistics records.

NOTE: **This topic describes the local file output in Junos OS Release 13.2X51-D15 and later. For information about local file output from earlier releases, see the monitor start (Analytics) topic.**

Beginning in Junos OS Release 13.2X51-D15, the traffic and queue monitoring statistics can be stored locally in a single file. The following example shows the output from the **monitor start** command.

```
root@qfx5100-33> monitor start an
root@qfx5100-33>
*** an ***
q,1393947567698432,qfx5100-33,xe-0/0/19,1098572,1373216
q,1393947568702418,qfx5100-33,xe-0/0/19,1094912,1368640
```


Copyright © 2018, Juniper Networks, Inc.

```
q,1393947569703415,qfx5100-33,xe-0/0/19,1103065,1378832
t,1393947569874528,qfx5100-33,xe-0/0/16,12603371884,12603371884,0,0,
8426023,1613231610488,8628248712,0,3,5916761,5916761,0,0,0,757345408,0,0,0
t,1393947569874528,qfx5100-33,xe-0/0/18,12601953614,12601953614,0,0,
8446737,1613050071660,8649421552,0,5,131761619,131761619,0,0,84468,
16865487232,86495888,0,0
t,1393947569874528,qfx5100-33,xe-0/0/19,126009250,126009250,0,0,84469,
16129184128,86496392,0,0,12584980342,12584980342,0,0,8446866,1610877487744,
8649588432,12593703960,0
q,1393947575698402,qfx5100-33,xe-0/0/19,1102233,1377792
q,1393947576701398,qfx5100-33,xe-0/0/19,1107724,1384656
```

See Table 18 on page 121 for queue statistics output, and Table 19 on page 121 for traffic statistics output. The fields in the tables are listed in the order they appear in the output example.

Table 18: Output Fields for Queue Statistics in Local Analytics File

Field	Description	Example in Output
Record type	Type of statistics (queue or traffic monitoring)	**q**
Time (microseconds)	Unix epoch (or Unix time) in microseconds at which the statistics were captured.	**1393947567698432**
Router ID	ID of the network analytics host device.	**qfx5100-33**
Port	Name of the physical port configured for network analytics.	**xe-0/0/19**
Latency (nanoseconds)	Traffic queue latency in nanoseconds.	**1098572**
Queue depth (bytes)	Depth of the traffic queue in bytes.	**1373216**

Table 19: Output Fields for Traffic Statistics in Local Analytics File

Field	Description	Example in Output
Record type	Type of statistics (queue or traffic monitoring)	**t**
Time (microseconds)	Unix epoch (or Unix time) in microseconds at which the statistics were captured.	**1393947569874528**
Router ID	ID of the network analytics host device.	**qfx5100-33**
Port	Name of the physical port configured for network analytics.	**xe-0/0/16**
rxpkt	Total packets received.	**12603371884**
rxucpkt	Total unicast packets received.	**12603371884**
rxmcpkt	Total multicast packets received.	**0**
rxbcpkt	Total broadcast packets received.	**0**

Copyright © 2018, Juniper Networks, Inc.

Table 19: Output Fields for Traffic Statistics in Local Analytics File *(continued)*

Field	Description	Example in Output
rxpps	Total packets received per second.	**8426023**
rxbyte	Total octets received.	**1613231610488**
rxbps	Total bytes received per second.	**8628248712**
rxdroppkt	Total incoming packets dropped.	**0**
rxcrcerr	CRC/Align errors received.	**3**
txpkt	Total packets transmitted.	**5916761**
txucpkt	Total unicast packets transmitted.	**5916761**
txmcpkt	Total multicast packets transmitted.	**0**
txbcpkt	Total broadcast packets transmitted.	**0**
txpps	Total packets transmitted per second.	**0**
txbyte	Total octets transmitted.	**757345408**
txbps	Bytes per second transmitted.	**0**
txdroppkt	Total transmitted packets dropped.	**0**
txcrcerr	CRC/Align errors transmitted.	**0**

Release History Table

Release	Description
13.2X51-D15	Beginning in Junos OS Release 13.2X51-D15, the traffic and queue monitoring statistics can be stored locally in a single file.

Related Documentation

- Network Analytics Overview on page 103
- analytics on page 138

Prototype File for the Google Protocol Buffer Stream Format

The Google Protocol Buffer (GBP) stream format is used for streaming monitoring statistics data to a remote collector in a single AnRecord message.

The **analytics.proto** file provides a template for the GBP stream format. This file can be used for writing your analytics server application.

Copyright © 2018, Juniper Networks, Inc.

To download the GPB prototype file, go to:

https://www.juniper.net/documentation/en_US/junos13.2/topics/reference/proto-files/analytics-proto.txt

Related Documentation

- Network Analytics Overview on page 103
- analytics on page 138
- *export-profiles*

Configuring Queue Monitoring

Network analytics queue monitoring provides visibility into the performance and behavior of the data center infrastructure. This feature collects data from the switch, analyzes the data using sophisticated algorithms, and captures the results in reports. You can use the reports to help troubleshoot problems, make decisions, and adjust resources as needed.

You enable queue monitoring by first defining a resource profile template, and then applying the profile to the system (for a global configuration) or to individual interfaces.

NOTE: You can configure queue monitoring on physical network interfaces only; logical interfaces and Virtual Chassis physical (VCP) interfaces are not supported.

NOTE: The procedure to configure queue monitoring on a QFX Series standalone switch requires Junos OS Release 13.2X51-D15 or later to be installed on your device.

To configure queue monitoring on a QFX Series standalone switch:

1. Configure the queue monitoring polling interval (in milliseconds) globally (for the system):

   [edit]
   set services analytics resource system polling-interval queue-monitoring *interval*

2. Configure a resource profile for the system, and enable queue monitoring:

   [edit]
   set services analytics resource-profiles *profile-name* queue-monitoring

3. Configure high and low values of the depth-threshold (in bytes) for queue monitoring in the system profile:

   [edit]
   set services analytics resource-profiles *profile-name* depth-threshold high *number* low *number*

For both high and low values, the range is from 1 to 1,250,000,000 bytes, and the default value is 0 bytes.

NOTE: You can configure either the depth-threshold or latency threshold for the system, but not both.

4. Apply the resource profile template to the system for a global configuration:

   [edit]
   set services analytics resource system resource-profile *profile-name*

5. Configure an interface-specific resource profile and enable queue monitoring for the interface:

   [edit]
   set services analytics resource-profiles *profile-name* queue-monitoring

6. Configure the latency-threshold (high and low values) for queue monitoring in the interface-specific profile:

   [edit]
   set services analytics resource-profiles *profile-name* latency-threshold high *number* low *number*

   For both high and low values, the range is from 1 to 100,000,000 nanoseconds, and the default value is 1,000,000 nanoseconds.

   NOTE: You can configure either the depth-threshold or latency threshold for interfaces, but not both.

7. Apply the resource profile template for interfaces to one or more interfaces:

   [edit]
   set services analytics resource interfaces *interface-name* resource-profile *profile-name*

   NOTE: If a conflict arises between the system and interface configurations, the interface-specific configuration supersedes the global (system) configuration.

Copyright © 2018, Juniper Networks, Inc.

Release History Table

Release	Description
13.2X51-D15	The procedure to configure queue monitoring on a QFX Series standalone switch requires Junos OS Release 13.2X51-D15 or later to be installed on your device.

Related Documentation

- Network Analytics Overview on page 103
- *Example: Configuring Enhanced Network Analytics Features*
- analytics on page 138

Configuring Traffic Monitoring

Network analytics queue monitoring provides visibility into the performance and behavior of the data center infrastructure. This feature collects data from the switch, analyzes the data using sophisticated algorithms, and captures the results in reports. You can use the reports to help troubleshoot problems, make decisions, and adjust resources as needed.

You enable traffic monitoring by first defining a resource profile template, and then applying the profile to the system (for a global configuration) or to individual interfaces.

NOTE: You can configure traffic monitoring on physical network interfaces only; logical interfaces and Virtual Chassis physical (VCP) interfaces are not supported.

NOTE: The procedure to configure traffic monitoring on a QFX Series standalone switch requires Junos OS Release 13.2X51-D15 or later to be installed on your device.

To configure traffic monitoring on a QFX Series standalone switch:

1. Configure the traffic monitoring polling interval (in seconds) for the system:

   [edit]
   set services analytics resource system polling-interval traffic-monitoring *interval*

2. Configure a resource profile for the system, and enable traffic monitoring in the profile:

   [edit]
   set services analytics resource-profiles *profile-name* traffic-monitoring

3. Apply the resource profile to the system for a global configuration:

   [edit]
   set services analytics resource system resource-profile *profile-name*

4. Configure a resource profile for interfaces, and enable traffic monitoring in the profile:

   [edit]
   set services analytics resource-profiles *profile-name* traffic-monitoring

   NOTE: If a conflict arises between the system and interface configurations, the interface-specific configuration supersedes the global (system) configuration.

5. Apply the resource profile template to one or more interfaces:

   [edit]
   set services analytics resource interfaces *interface-name* resource-profile *profile-name*

Release History Table

Release	Description
13.2X51-D15	The procedure to configure traffic monitoring on a QFX Series standalone switch requires Junos OS Release 13.2X51-D15 or later to be installed on your device.

Related Documentation

- Network Analytics Overview on page 103
- *Example: Configuring Enhanced Network Analytics Features*
- analytics on page 138

Configuring a Local File for Network Analytics Data

The network analytics feature provides visibility into the performance and behavior of the data center infrastructure. This feature collects data from the switch, analyzes the data using sophisticated algorithms, and captures the results in reports. Network administrators can use the reports to help troubleshoot problems, make decisions, and adjust resources as needed.

To save the queue and traffic statistics data in a local file, you must configure a filename to store it.

NOTE: The procedure to configure a local file for storing queue and traffic monitoring statistics requires Junos OS Release 13.2X51-D15 or later to be installed on your device.

To configure a local file for storing queue and traffic monitoring statistics:

1. Configure a filename:

   [edit]
   set services analytics collector local file *filename*

Copyright © 2018, Juniper Networks, Inc.

There is no default filename. If you do not configure a filename, network analytics statistics are not saved locally.

2. Configure the number of files (from 2 to 1000 files):

   [edit]
   set services analytics collector local file *filename* files *number*

3. Configure the file size (from 10 to 4095 MB) in the format of *x*m:

   [edit]
   set services analytics collector local file an size *size*

Release History Table

Release	Description
13.2X51-D15	The procedure to configure a local file for storing queue and traffic monitoring statistics requires Junos OS Release 13.2X51-D15 or later to be installed on your device.

Related Documentation

- Network Analytics Overview on page 103
- *Example: Configuring Enhanced Network Analytics Features*
- analytics on page 138

Configuring a Remote Collector for Streaming Analytics Data

The network analytics feature provides visibility into the performance and behavior of the data center infrastructure. This feature collects data from the switch, analyzes the data using sophisticated algorithms, and captures the results in reports. Network administrators can use the reports to help troubleshoot problems, make decisions, and adjust resources as needed.

You can configure an export profile to define the stream format and type of data, and one or more remote servers (collectors) to receive streaming network analytics data.

NOTE: **The procedure to configure a collector for receiving streamed analytics data requires Junos OS Release 13.2X51-D15 or later to be installed on your device.**

To configure a collector for receiving streamed analytics data:

1. Create an export profile and specify the stream format:

   [edit]
   set services analytics export-profiles *profile-name* stream-format *format*

2. Configure the export profile to include interface information:

```
[edit]
set services analytics export-profiles profile-name interface information
```

3. Configure the export profile to include interface queue statistics:

```
[edit]
set services analytics export-profiles profile-name interface statistics queue
```

4. Configure the export profile to include interface traffic statistics:

```
[edit]
set services analytics export-profiles profile-name interface statistics traffic
```

5. Configure the export profile to include interface status link information:

```
[edit]
set services analytics export-profiles profile-name interface status link
```

6. Configure the export profile to include system information:

```
[edit]
set services analytics export-profiles profile-name system information
```

7. Configure the export profile to include system queue status:

```
[edit]
set services analytics export-profiles profile-name system status queue
```

8. Configure the export profile to include system traffic status:

```
[edit]
set services analytics export-profiles profile-name system status traffic
```

9. Configure the transport protocol for the collector addresses and apply the export profile:

```
[edit]
set services analytics collector address ip-address port port transport protocol
  export-profile profile-name
set services analytics collector address ip-address port port transport protocol
  export-profile profile-name
```

NOTE: If you configure the tcp or udp option for the JSON, CSV, and TSV formats, you must also set up the TCP or UDP client software on the remote collector to process records that are separated by the newline character (\n) on the remote server.

If you configure the tcp or udp option for the GPB format, you must also set up the TCP or UDP build streaming server using the analytics.proto file.

Copyright © 2018, Juniper Networks, Inc.

Release History Table

Release	Description
13.2X51-D15	The procedure to configure a collector for receiving streamed analytics data requires Junos OS Release 13.2X51-D15 or later to be installed on your device.

Related Documentation

- Network Analytics Overview on page 103
- *Example: Configuring Enhanced Network Analytics Features*
- **analytics on page 138**

Example: Configuring Network Analytics

This example shows how to configure network analytics which includes queue and traffic monitoring on a QFX3500 standalone switch.

NOTE: **The configuration shown in this example is supported only on Junos OS Release 13.2X50-D15 and 13.2X51-D10.**

- Requirements on page 129
- Overview on page 130
- Configuration on page 130
- Verification on page 133

Requirements

This example uses the following hardware and software components:

- A QFX3500 standalone switch
- A external streaming server to collect data
- Junos OS Release 13.2X50-D15 software
- TCP server software (for remote streaming servers)

Before you configure network analytics, be sure you have:

- Junos OS Release 13.2X50-D15 or later software installed and running on the QFX3500 switch
- (Optional for streaming servers) TCP server software set up for processing records separated by a newline character (\n) on the remote streaming server
- All other devices running

Overview

The network analytics feature provides visibility into the performance and behavior of the data center infrastructure. This feature collects data from the switch, analyzes the data using sophisticated algorithms, and captures the results in reports. Network administrators can use the reports to help troubleshoot problems, make decisions, and adjust resources as needed. You can enable network analytics by configuring queue and traffic statistics monitoring.

Topology

In this example, the QFX3500 switch is connected to an external server used for streaming statistics data.

Configuration

To configure network analytics, perform these tasks:

- Configuring Queue and Traffic Statistics Monitoring on page 131
- Configuring Local Statistics Files on page 131
- Configuring Streaming Servers on page 132
- Results on page 132

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
[edit]
set services analytics interfaces all queue-statistics
set services analytics interfaces all latency-threshold high 900 low 300
set services analytics interfaces xe-0/0/1 traffic-statistics
set services analytics queue-statistics file qstats1.qs files 3 size 10
set services analytics queue-statistics interval 10
set services analytics traffic-statistics file tstats1.ts files 3 size 10
set services analytics traffic-statistics interval 2
set services analytics streaming-servers address 10.94.198.11 port 50001 stream-format
   json stream-type queue-statistics
set services analytics streaming-servers address 10.94.198.11 port 50005 stream-format
   csv stream-type traffic-statistics
```


Copyright © 2018, Juniper Networks, Inc.

Configuring Queue and Traffic Statistics Monitoring

Step-by-Step Procedure

To configure queue and traffic monitoring on physical interfaces:

NOTE: You can configure queue and traffic monitoring on physical network interfaces only; logical interfaces and Virtual Chassis physical (VCP) interfaces are not supported.

NOTE: Disabling of the queue or traffic monitoring supersedes the configuration (enabling) of this feature. You disable monitoring by issuing the **no-queue-statistics** or **no-traffic-statistics** at the **[edit services analytics interfaces]** hierarchy level.

1. Configure all interfaces for queue monitoring and set the latency thresholds (in microseconds):

   [edit]
   set services analytics interfaces all queue-statistics
   set services analytics interfaces all latency-threshold high 900 low 300

2. Configure one interface for traffic monitoring:

   [edit]
   set services analytics interfaces xe-0/0/1 traffic-statistics

Configuring Local Statistics Files

Step-by-Step Procedure

To configure local statistics files:

1. Configure the number of queue statistics files, and each file size in MB:

   [edit]
   set services analytics queue-statistics file qstats1.qs files 3 size 10m

2. Configure the queue statistics collection interval in milliseconds

   [edit]
   set services analytics queue-statistics interval 10

3. Configure the number of traffic statistics files, and each file size in MB:

   [edit]
   set services analytics traffic-statistics file tstats1.ts files 3 size 10m

4. Configure the traffic statistics collection interval in seconds:

```
[edit]
set services analytics traffic-statistics interval 2
```

Configuring Streaming Servers

Step-by-Step Procedure

To configure streaming servers for receiving monitoring data:

NOTE: In addition to configuring streaming servers, you must also set up the TCP client software to process records that are separated by the newline character (\n) on the remote server.

1. Configure a server IP address and port for queue statistics monitoring:

```
[edit]
set services analytics streaming-servers address 10.94.198.11 port 50001
  stream-format json stream-type queue-statistics
```

2. Configure a server IP address and port for traffic statistics monitoring:

```
[edit]
set services analytics streaming-servers address 10.94.198.11 port 50005
  stream-format csv stream-type traffic-statistics
```

Results

Display the results of the configuration:

```
[edit services analytics]
user@switch> show configuration
  queue-statistics {
    file qstats1.qs size 10m files 3;
    interval 10;
  }
  traffic-statistics {
    file tstats1.ts size 10m files 3;
    interval 2;
  }
  interfaces {
    xe-0/0/1 {
      traffic-statistics;
    }
    all {
      queue-statistics;
      latency-threshold high 900 low 300;
    }
  }
```


Copyright © 2018, Juniper Networks, Inc.

Verification

Confirm that the configuration is correct and works as expected by performing these tasks:

- Verifying the Network Analytics Configuration on page 133
- Verifying the Network Analytics Status on page 133
- Verifying Streaming Servers Configuration on page 134
- Verifying Queue Statistics on page 134
- Verifying Traffic Statistics on page 135

Verifying the Network Analytics Configuration

Purpose Verify the configuration for network analytics.

Action From operational mode, enter the **show analytics configuration** command to display the traffic and queue monitoring configuration.

```
user@host> show analytics configuration
Global configurations:
   Traffic statistics: Auto, Poll interval: 2 seconds
   Queue statistics: Enabled, Poll interval: 10 milliseconds
   Depth threshold high: 0 bytes, low: 0 bytes
   Latency threshold high: 900 microseconds, low: 300 microseconds
Interface     Traffic       Queue        Depth-threshold      Latency-threshold
            Statistics    Statistics      High      Low         High      Low
                                             (bytes)            (microseconds)
xe-0/0/1     Enabled      Auto            0         0           900       300
```

Meaning The output displays information about traffic and queue monitoring on the switch.

Verifying the Network Analytics Status

Purpose Verify the network analytics operational status of the switch.

Action From operational mode, enter the **show analytics status** command to display the traffic and queue monitoring status.

```
user@host> show analytics status
Global configurations:
   Traffic statistics: Auto, Poll interval: 2 seconds
   Queue statistics: Auto, Poll interval: 10 milliseconds
   Depth threshold high: 1228800 bytes, low: 1024 bytes
   Latency threshold high: 900 microseconds, low: 300 microseconds
Interface     Traffic       Queue        Depth-threshold      Latency-threshold
            Statistics    Statistics      High      Low         High      Low
                                            (bytes)            (microseconds)
xe-0/0/1     Enabled       Auto          1228800   1024         900       300
xe-0/0/7     Auto          Auto          1228800   1024         900       300
xe-0/0/8     Auto          Auto          1228800   1024         900       300
```

Verifying Streaming Servers Configuration

Purpose Verify the configuration for streaming data to remote servers is working.

Action From operational mode, enter the **show analytics streaming-servers** command to display the streaming servers configuration.

```
user@host> show analytics streaming-servers
Address        Port     Stream-Format    Stream-Type   State         Sent
10.94.198.11   50001    json             QS            Established   1100
10.94.198.11   50005    csv              TS/QS         In Progress      0
```

Meaning The output displays information about the remote streaming server.

Verifying Queue Statistics

Purpose Verify that queue statistics collection is working.

Action From operational mode, enter the **show analytics queue-statistics** command to display the queue statistics.

```
user@host> show analytics queue-statistics
Time               Interface   Queue-length (bytes)   Latency (us)
Apr 6 0:17:18.224  xe-0/0/1            1043952            835
Apr 6 0:17:18.234  xe-0/0/1            1053520            842
Apr 6 0:17:18.244  xe-0/0/1            1055184            844
```

Meaning The output displays queue-statistics information as expected.

Copyright © 2018, Juniper Networks, Inc.

Verifying Traffic Statistics

Purpose Verify that traffic statistics collection is working.

Action From operational mode, enter the **show analytics traffic-statistics** command to display the traffic statistics.

```
user@host> show analytics traffic-statistics
Time: Apr 5 19:52:48.549, Physical interface: xe-0/0/1
  Traffic Statistics:                Receive            Transmit
  Total octets:                4797548752936        408886273632
  Total packet:                   5658257464          3190613435
  Octets per second:                       0                   0
  Packet per second:                       0                   0
  Octets dropped:                          0           252901000
  Packet dropped:                          0              252901
  Utilization:                          0.0%                0.0%
Time: Apr 5 19:52:48.549, Physical interface: xe-0/0/7
  Traffic Statistics:                Receive            Transmit
  Total octets:                4790866253100           477139024
  Total packet:                   5624473639              477944
  Octets per second:                       0                   0
  Packet per second:                       0                   0
  Octets dropped:                          0           166582000
  Packet dropped:                          0              166582
  Utilization:                          0.0%                0.0%
Time: Apr 5 19:52:48.549, Physical interface: xe-0/0/8
  Traffic Statistics:                Receive            Transmit
  Total octets:                4789797668456           764910024
  Total packet:                   5623280870              765715
  Octets per second:                       0                   0
  Packet per second:                       0                   0
  Octets dropped:                          0           156099000
  Packet dropped:                          0              156099
  Utilization:                          0.0%                0.0%
```

Meaning The output displays traffic-statistics information as expected.

Related Documentation

- Network Analytics Overview on page 103
- analytics on page 138
- show analytics status on page 167
- show analytics streaming-servers on page 171

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 8

Network Analytics Configuration Statements

- analytics on page 138
- depth-threshold on page 142
- interfaces (Analytics) on page 144
- latency-threshold on page 146
- queue-statistics on page 148
- streaming-servers on page 150
- traceoptions (Analytics) on page 152
- traffic-statistics on page 153

Copyright © 2018, Juniper Networks, Inc.

analytics

Syntax *Junos OS Release 13.2X51-D15 and later:*

```
analytics {
  collector {
    local {
      file filename {
        size size;
        files number;
      }
    }
    address ip-address {
      port number {
        transport protocol {
          export-profile profile-name;
        }
      }
    }
  }
  export-profiles {
    profile-name {
      interface {
        information;
        statistics {
          queue;
          traffic;
        }
        status {
          link;
          queue;
          traffic;
        }
      }
      stream-format format;
      system {
        information;
        status {
          queue;
          traffic;
        }
      }
    }
  }
  resource {
    interfaces {
      interface-name {
        resource-profile name;
      }
    }
    system {
      polling-interval {
        queue-monitoring interval;
        traffic-monitoring interval;
      }
```

 Copyright © 2018, Juniper Networks, Inc.

```
            resource-profile name;
        }
    }
    resource-profiles {
        profile-name {
            depth-threshold {
                high number;
                low number;
            }
            latency-threshold {
                high number;
                low number;
            }
            no-queue-monitoring;
            no-traffic-monitoring;
            queue-monitoring;
            traffic-monitoring;
        }
    }
    traceoptions {
        file filename {
            files number;
            size size;
        }
    }
}
```

Junos OS Release 13.2X50-D15 and 13.2X51-D10 only:

```
analytics {
  interfaces {
    all {
      depth-threshold high number low number;
      latency-threshold high number low number;
      queue-statistics;
      no-queue-statistics;
      traffic-statistics;
      no-traffic-statistics;
    }
    interface-name {
      depth-threshold high number low number;
      latency-threshold high number low number;
      queue-statistics;
      no-queue-statistics;
      traffic-statistics;
      no-traffic-statistics;
    }
  }
  queue-statistics {
    file filename {
      files number-of-files;
      size size;
    }
    interval interval;
  }
  streaming-servers {
    address ip-address {
      port number {
        stream-format format;
        stream-type type
      }
    }
  }
  traceoptions {
    file filename {
      files number;
      size size;
    }
  }
  traffic-statistics {
    file filename {
      files number-of-files;
      size size;
    }
    interval interval;
  }
}
```

Hierarchy Level [edit services]

 Copyright © 2018, Juniper Networks, Inc.

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

Configure the network analytics feature that includes monitoring for traffic and queue statistics. The network analytics processes running on the Packet Forwarding Engine and Routing Engine collect and analyze the data, and generate reports that may be saved in log files or sent as streaming data to remote servers.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Network Analytics Overview on page 103
- show analytics traffic-statistics on page 173
- show analytics collector on page 159
- show analytics status on page 167
- show analytics queue-statistics on page 165
- show analytics configuration on page 161

Copyright © 2018, Juniper Networks, Inc.

depth-threshold

Syntax

```
depth-threshold {
   high number;
   low number;
}
```

Hierarchy Level

[edit services analytics interfaces]
[edit services analytics resource-profiles]

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement in the **[edit services analytics resource-profiles]** hierarchy level introduced in Junos OS Release 13.2X51-D15.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

If network analytics queue statistics monitoring is enabled, specify the high and low values (in bytes) of the queue depth (buffer) threshold. If you configure a depth threshold, you cannot configure the latency threshold. You can configure the depth threshold for one interface or all interfaces. Specify the high and low queue depth threshold numbers:

NOTE: **The configuration for a specific interface supersedes the global configuration for all interfaces.**

Options

high *number*—Specify the maximum value for the depth threshold.

Range: 1 to 1,250,000,000 bytes

Default:

- Junos OS Release 13.2X51-D10 or later—0 bytes
- Junos OS Release 13.2X50-D15—14,680,064 bytes (14 MB)

low *number*—Specify the minimum value for the depth threshold.

Range: 1 to 1,250,000,000 bytes

Default:

- Junos OS Release 13.2X51-D10 or later—0 bytes
- Junos OS Release 13.2X50-D15—1024 bytes (1 KB)

Required Privilege Level

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

Related Documentation

- Network Analytics Overview on page 103
- analytics on page 138

Copyright © 2018, Juniper Networks, Inc.

- latency-threshold on page 146
- *resource-profiles (Analytics)*

interfaces (Analytics)

Syntax

```
interfaces {
  all {
    depth-threshold high number low number;
    latency-threshold high number low number;
    queue-statistics;
    no-queue-statistics;
    traffic-statistics;
    no-traffic-statistics;
  }
  interface-name {
    depth-threshold high number low number;
    latency-threshold high number low number;
    queue-statistics;
    no-queue-statistics;
    traffic-statistics;
    no-traffic-statistics;
  }
}
```

Hierarchy Level [edit services analytics]

Release Information Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description Configure physical interfaces for monitoring traffic and queue statistics by the network analytics processes running on the Packet Forwarding Engine and Routing Engine. You may specify one interface or all interfaces in your configuration.

NOTE: The configuration for a specific interface supersedes the global configuration for all interfaces. You can configure traffic and queue monitoring for physical interfaces only; logical interfaces and Virtual Chassis port (VCP) interfaces are not supported.

NOTE: Disabling the queue or traffic monitoring (using the **no-queue-statistics** or **no-traffic-statistics** configuration statements) supersedes the configuration (enabling) of the feature.

Options **all**—Configure all interfaces on the device for high-frequency monitoring.

interface-name—Name of the interface to configure for high-frequency monitoring.

no-queue-statistics—Disable the collection of queue statistics.

Copyright © 2018, Juniper Networks, Inc.

NOTE: The **no-queue-statistics** statement supersedes the **queue-statistics** statement.

no-traffic-statistics—Disable the collection of traffic statistics.

NOTE: The **no-traffic-statistics** statement supersedes the **traffic-statistics** statement.

queue-statistics—Enable the collection of queue statistics for a specific interface or all interfaces.

traffic-statistics—Enable the collection of traffic statistics for a specific interface or all interfaces.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Network Analytics Overview on page 103
- analytics on page 138

latency-threshold

Syntax

```
latency-threshold {
   high number;
   low number;
}
```

Hierarchy Level

[edit services analytics interfaces]
[edit services analytics resource-profiles]

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement in the **[edit services analytics resource-profiles]** hierarchy level introduced in Junos OS Release 13.2X51-D15.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

If network analytics queue statistics monitoring is enabled, specify the high and low values (in microseconds) of the latency threshold of the queue. If you configure a latency threshold, you cannot configure the depth threshold. You can configure the latency threshold for one interface or all interfaces. Specify the high and low latency threshold numbers:

NOTE: **The configuration for a specific interface supersedes the global configuration for all interfaces.**

Options

high *number*—Specify the maximum value for the latency threshold.

Range:

- Junos OS Release 13.2X51-D15 or later—1 to 100,000,000 nanoseconds (0.001 to 100,000 microseconds)
- Junos OS Release 13.2X51-D10 or earlier—1 to 100,000 microseconds

Default:

- Junos OS Release 13.2X51-D15 or later—1,000,000 nanoseconds (1000 microseconds or 1 millisecond)
- Junos OS Release 13.2X51-D10—1000 microseconds
- Junos OS Release 13.2X50-D15—900 microseconds

low *number*—Specify the minimum value for the latency threshold.

Range:

- Junos OS Release 13.2X51-D15 or later—1 to 100,000,000 nanoseconds
- Junos OS Release 13.2X51-D10 or earlier—1 to 100,000 microseconds

Default:

Copyright © 2018, Juniper Networks, Inc.

- Junos OS Release 13.2X51-D15 or later—100 nanoseconds (0.1 microseconds)
- Junos OS Release 13.2X51-D10—50 microseconds
- Junos OS Release 13.2X50-D15—300 microseconds

Required Privilege Level

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

Related Documentation

- Network Analytics Overview on page 103
- **analytics on page 138**
- **depth-threshold on page 142**

queue-statistics

Syntax

```
queue-statistics {
  file filename {
    files number-of-files;
    size size;
  }
  interval interval;
}
```

Hierarchy Level [edit services analytics]

Release Information Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description Enable the logging of queue statistics in a local file. This statement does not enable queue statistics monitoring.

To enable queue monitoring, you must specify the **queue-statistics** configuration statement at the **[edit services analytics interfaces]** hierarchy level.

Default This feature is disabled by default.

Options **interval *interval***—Configure the polling interval in milliseconds.

NOTE: You can configure the polling interval for queue statistics globally for all interfaces only. Due to limitations and variations in the hardware capability of different devices, you might see a difference in value between the actual interval and configured interval.

Range:

- Junos OS Release 13.2X50-D15—8 to 1000 milliseconds (8 milliseconds to 1 second)
- Junos OS Release 13.2X51-D10 or later—10 to 1000 milliseconds (10 milliseconds to 1 second)

NOTE: In Junos OS Release 13.2X51-D10 or later, if you configured an interval of less than 10 milliseconds, the following warning messages appear during the commit process: **Queue statistics polling interval can not be less than 10 milliseconds** and **Setting Queue statistics polling interval to 10 milliseconds**. These messages do not stop the commit operation, but the interval is automatically set to 10 milliseconds.

Copyright © 2018, Juniper Networks, Inc.

Default:

- Junos OS Release 13.2X50-D15—8 milliseconds
- Junos OS Release 13.2X51-D10 or later—10 milliseconds

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Network Analytics Overview on page 103
- analytics on page 138

streaming-servers

Syntax

```
streaming-servers {
   address ip-address {
      port number {
         stream-format format;
         stream-type type
      }
   }
}
```

Hierarchy Level [edit services analytics]

Release Information Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description Configure remote servers to receive streaming output for the network analytics monitoring of traffic and queue statistics. The streaming function supports TCP connections only, and sends records separated by a newline character.

NOTE: **Before you use the remote server to receive streaming data, you must set up the TCP server software to process records that are separated by the newline character (\n).**

You can configure multiple servers and multiple ports on each server to receive the streaming data. You can configure different streaming data types and formats for different ports on a server, but you can configure only one streaming type and one format for each port on a server.

Options

address *ip-address*—IP address of the remote server receiving the streaming data.

port *number*—Port number of the remote server receiving the streaming data.

stream-format *format*—Format of the streaming data being sent to a server. Only one format can be sent to each port on a server.

Values:

- **csv**—Comma-separated Values (CSV). Records sent in this format contain a “q” for a queue statistics, or a “t” for a traffic statistics.
- **json**—JavaScript Object Notification (JSON). Records sent in this format contain “queue-statistics” or “traffic-statistics” in the “record type” field.
- **tsv**—Tab-separated Values (TSV). Records sent in this format contain a “q” for a queue statistics, or a “t” for a traffic statistics.

stream-type *type*—Type of streaming data sent to a port. You can specify different types of streaming data to be sent to different ports on the same server.

Copyright © 2018, Juniper Networks, Inc.

Values:

- **queue-statistics**
- **traffic-statistics**

Required Privilege Level

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

Related Documentation

- Network Analytics Overview on page 103
- Understanding Network Analytics Streaming Data on page 112
- **analytics on page 138**

traceoptions (Analytics)

Syntax

```
traceoptions {
   file filename;
   files number-of-files;
   size size;
}
```

Hierarchy Level

[edit services analytics]

Release Information

Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

Configure traceoptions for the network analytics daemon (analyticsd) running on the Routing Engine.

Options

file *filename*—Specify a filename for storing the traceoptions data. The file is stored in the **/var/log/** directory of your device.

If you do not specify a filename, the data is not stored in a file.

files *number-of-files*—Specify the number of files to store locally. After the number files witsh the maximum file size is reached, the system starts over and writes the data to the first file.

Range: 2 to 1,000 files.

size *size*—Configure the file size in megabytes (MB).

Syntax: ***x*m** to specify MB.

Range: 10 to 4095 MB

Required Privilege Level

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

Related Documentation

- Network Analytics Overview on page 103
- analytics on page 138

Copyright © 2018, Juniper Networks, Inc.

traffic-statistics

Syntax

```
traffic-statistics {
   file filename {
      files number-of-files;
      size size;
   }
   interval interval;
}
```

Hierarchy Level [edit services analytics]

Release Information Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description Enable the logging of traffic statistics in a local file. This statement does not enable traffic statistics monitoring.

To enable the monitoring of traffic statistics, configure the **traffic-statistics** configuration statement at the **[edit services analytics interfaces]** hierarchy level.

Default This feature is disabled by default.

Options

file *filename*—Specify a filename for storing the traffic statistics in the JavaScript Object Notification (JSON) format. The file is stored in the **/var/log/** directory of your device.

If you do not specify a filename, the data is not stored in a file.

files *number-of-files*—Specify the number of files to store locally. After the number files with the maximum file size is reached, the system starts over and writes the data to the first file.

Range: 2 to 1,000 files.

interval *interval*—Configure the polling interval in seconds.

NOTE: You can configure the polling interval for traffic statistics globally for all interfaces only. Due to limitations and variations in the hardware capability of different devices, you might see a difference in value between the actual interval and configured interval.

Range:

- Junos OS Release 13.2X51-D10 or later—2 to 300 seconds (2 seconds to 5 minutes)
- Junos OS Release 13.2X50-D15—1 to 300 seconds (1 second to 5 minutes)

NOTE: In Junos OS Release 13.2X51-D10 or later, if you configured an interval of less than 2 seconds, the following warning messages appear during the commit process:

Traffic statistics polling interval can not be less than 2 seconds, and

Setting Traffic statistics polling interval to 2 seconds.

These messages do not stop the commit operation, but the interval is automatically set to 2 seconds.

Default:

- Junos OS Release 13.2X50-D15—1 second
- Junos OS Release 13.2X51-D10 or later—2 seconds

size *size*—Configure the file size in megabytes (MB).

Syntax: ***x*m** to specify MB.

Range: 10 to 4095 MB

Required Privilege Level

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

Related Documentation

- Network Analytics Overview on page 103
- **analytics on page 138**

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 9

Network Analytics Operational Commands

- monitor start (Analytics)
- show analytics collector
- show analytics configuration
- show analytics queue-statistics
- show analytics status
- show analytics streaming-servers
- show analytics traffic-statistics

Copyright © 2018, Juniper Networks, Inc.

monitor start (Analytics)

Syntax monitor start *filename*

Release Information Command introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description Start the display of the queue statistics or traffic statistics file if you had enabled queue or traffic monitoring on your device. The output is displayed in the JavaScript Object Notation (JSON) format.

NOTE: **This topic describes the local file output in Junos OS Release 13.2X50-D15 and 13.2X51-D10 only. For information about 13.2X51-D15 and later, see** "Understanding Enhanced Analytics Local File Output" on page 120

Options ***filename***—Name of the queue statistics or traffic statistics file.

Required Privilege Level trace

Related Documentation

- Network Analytics Overview on page 103
- analytics on page 138

List of Sample Output

monitor start Using the Queue Statistics File (Junos OS Release 13.2X51-D10) on page 157
monitor start Using the Queue Statistics File (Junos OS Release 13.2X50-D15) on page 158
monitor start Using the Traffic Statistics File (Junos OS Release 13.2X51-D10) on page 158
monitor start Using the Traffic Statistics File (Junos OS Release 13.2X50-D15) on page 158

Output Fields Table 20 on page 156 describes the output fields for the **monitor start** command. Output fields are listed in the approximate order in which they appear.

Table 20: monitor start Command Output Fields

Field	Description
hostname (used in Junos OS Release 13.2X50-D15 only)	Name of the network analytics host device.
record type	Type of statistics. May be queue statistics or traffic statistics.

 Copyright © 2018, Juniper Networks, Inc.

Table 20: monitor start Command Output Fields *(continued)*

Field	Description
time	Time at which the statistics were captured.
router-id	ID of the network analytics host device.
latency	For queue statistics only. Traffic queue latency in milliseconds.
port	Name of the physical port configured for network analytics.
queue depth	For queue statistics only. Depth of the traffic queue in bytes.
rxpkt	For traffic statistics monitoring only. Total packets received.
rxpps	For traffic statistics monitoring only. Total packets received per second.
rxbyte	For traffic statistics monitoring only. Total bytes received.
rxbps	For traffic statistics monitoring only. Total bytes received per second.
rxdrop	For traffic statistics monitoring only. Total incoming packets dropped.
rxerr	For traffic statistics monitoring only. Total packets with errors.
rxutil (in Junos OS Release 13.2X50-D15 only)	For traffic statistics monitoring only. Total percent of traffic utilization for incoming traffic.
txpkt	For traffic statistics monitoring only. Total packets transmitted.
txpps	For traffic statistics monitoring only. Total packets transmitted per second.
txbyte	For traffic statistics monitoring only. Total bytes transmitted.
txbps	For traffic statistics monitoring only. Total bytes transmitted per second.
txdrop	For traffic statistics monitoring only. Total transmitted bytes dropped.
txerr	For traffic statistics monitoring only. Total transmitted packets with errors (dropped).
txutil (in Junos OS Release 13.2X50-D15 only)	For traffic statistics monitoring only. Total percent of traffic utilization for outgoing traffic.

Sample Output

monitor start Using the Queue Statistics File (Junos OS Release 13.2X51-D10)

```
user@host> monitor start analytics.qs
{"record-type":"queue-stats","time":"2013 Nov 3 4:40:42.840",
"router-id":"qfx5100-switch","port":"xe-0/0/18","latency":0,"queue-depth":208}
```

```
{"record-type":"queue-stats","time":"2013 Nov 3 4:40:44.887",
"router-id":"qfx5100-switch","port":"xe-0/0/18","latency": 1110,"queue-depth":
1387568}
```

monitor start Using the Queue Statistics File (Junos OS Release 13.2X50-D15)

```
user@host> monitor start analytics.qs
{"hostname":"sw-la-pb-03","latency":566,"port":xe-0/0/9,"queue depth":708656,
"record type":"queue-stats","time":"Apr 11 20:18:40.329"}
```

Sample Output

monitor start Using the Traffic Statistics File (Junos OS Release 13.2X51-D10)

```
user@host> monitor start analytics.ts
{"record-type":"traffic-stats","time":"2013 Nov 3 4:39:53.910",
"router-id":"qfx5100-switch","port":"xe-0/0/18","rxpkt":23193749091,"rxpps":8299889,

"rxbyte":2968799876957,"rxbps":824002992,"rxdrop":0,"rxerr":0,"txpkt":1029323986,
"txpps":82671,"txbyte":131753470470,"txbps":85598256,"txdrop":0,"txerr":0}
```

monitor start Using the Traffic Statistics File (Junos OS Release 13.2X50-D15)

```
user@host> monitor start analytics.ts
{"hostname":"sw-la-pb-03","port":"xe-0/0/9","record type":"traffic-statistics",
"time":"Apr 11 20:13:48.545", "rxpkt":601024640, "rxpps": 840315,
"rxbyte":76931153920,
"rxbps":863997032, "rxdrop":0, "rxerr":0, "rxutil":8.32,"txpkt":336551380309,
"txpps":405395,"txbyte":23369872265951,"txbps":3240000976,"txdrop":1010566660824,
"txerr":69920099883860,"txutil":32.76}
```


Copyright © 2018, Juniper Networks, Inc.

show analytics collector

Syntax show analytics collector

Release Information Command introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description Show the list of network analytics remote collectors and related information. Remote collectors can be configured to receive streaming output for queue statistics and traffic statistics from the network analytics process (Analyticsd) running on the Routing Engine.

NOTE: The **show analytics collector** command is not available in Junos OS Releases prior to 13.2X51-D15.

Required Privilege Level interface-control

Related Documentation

- Network Analytics Overview on page 103
- **analytics on page 138**
- *address (Analytics Collector)*

List of Sample Output **show analytics collector on page 160**

Output Fields Table 21 on page 159 describes the output fields for the **show analytics collector** command.

Table 21: show analytics collector Command Output Fields

Field	Description
Address	IP Address of the collector that is configured for receiving the streaming data.
Port	Port number of the collector receiving the streaming data.
Transport	Transport protocol: • tcp—Transmission Control Protocol • udp—User Datagram Protocol NOTE: The connection state of a port configured with the **udp** transport protocol is always displayed as **n/a**.

Table 21: show analytics collector Command Output Fields *(continued)*

Field	Description
Stream format	Format of the data that is sent to the server: • csv—Comma-separated values • gpb—Google Protocol Buffer • json—JavaScript Object Notation • tsv—Tab-separated values
State	Connection state of the streaming server.
Sent	Number of bytes sent to the streaming server.

Sample Output

show analytics collector

```
user@host> show analytics collector
Address        Port   Transport  Stream format  State            Sent
10.94.184.25   50013  udp        gpb            n/a              8710
10.94.184.25   50040  tcp        gpb            Not initialized  0
10.94.184.25   50050  tcp        gpb            Established      405
10.94.184.62   50010  tcp        csv            Established      18
10.94.184.62   50020  udp        json           n/a              17
```


Copyright © 2018, Juniper Networks, Inc.

show analytics configuration

Syntax show analytics configuration

Release Information Command introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description Show the network analytics configuration details for the global and interface configurations.

Required Privilege Level interface-control

Related Documentation
- Network Analytics Overview on page 103
- analytics on page 138

List of Sample Output show analytics configuration (Junos OS Release 13.2X51-D15 and Later) on page 164
show analytics configuration (Junos OS Release 13.2X51-D10 and Earlier) on page 164

Output Fields describes the output fields for the **show analytics configuration** command in Junos OS Release 13.2X51-D15 and later.

Table 22: show analytics configuration Command Output Fields (Junos OS Release 13.2X51-D15 and Later)

Field	Descriptions
Global Configurations	
Traffic monitoring status	Settings are enabled or disabled. If traffic statistics monitoring is not enabled, this field is not shown.
Traffic monitoring polling interval	Interval for traffic statistics polling in seconds. NOTE: Due to limitations and variations in hardware capability in different devices, there might be a difference in value between the actual interval and configured interval.
Queue monitoring status	Settings are enabled or disabled. If queue statistics monitoring is not enabled, this field is not shown.
Queue monitoring polling interval	Interval for queue statistics polling in milliseconds. NOTE: Due to limitations and variations in hardware capability in different devices, there might be a difference in value between the actual interval and configured interval.
Queue depth high threshold	Upper limit of the depth threshold configuration in number of bytes. If the queue depth threshold is not configured, this field is not shown.

Table 22: show analytics configuration Command Output Fields (Junos OS Release 13.2X51-D15 and Later) *(continued)*

Field	Descriptions
Queue depth low threshold	Lower limit of the depth threshold configuration in number of bytes. If the queue depth threshold is not configured, this field is not shown.
Queue latency high threshold	Upper limit of the latency threshold configuration in nanoeconds. If the queue latency threshold is not configured, this field is not shown.
Queue latency low threshold	Lower limit of the latency threshold configuration in microseconds. If the queue latency threshold is not configured, this field is not shown.
Interface Configurations	
Interface	Name of interface that is configured for network analytics. The interface configuration overrides the global network analytics configuration.
Traffic Statistics	Settings are Enabled or Disabled for the interface.
Queue Statistics	Settings are Enabled or Disabled for the interface.
Queue depth threshold High	Upper limit of the depth threshold configuration in number of bytes. If the queue depth threshold is not configured, **n/a** is displayed.
Queue depth threshold Low	Lower limit of the depth threshold configuration in number of bytes. If the queue depth threshold is not configured, **n/a** is displayed.
Latency threshold High	Upper limit of the latency threshold configuration in nanoseconds. If the latency threshold is not configured, **n/a** is displayed.
Latency threshold Low	Lower limit of the latency threshold configuration in nanoseconds. If the latency threshold is not configured, **n/a** is displayed.

Table 23 on page 162 describes the output fields for the **show analytics configuration** command in Junos OS Release 13.2X51-D10 and 13.2X50-D15.

Table 23: show analytics configuration Command Output Fields (Junos OS Release 13.2X51-D10 and earlier)

Field	Descriptions
Global Configurations	
Traffic statistics	Settings are Auto, Enabled, or Disabled. If **Auto** is displayed, traffic statistics monitoring is not enabled.

Copyright © 2018, Juniper Networks, Inc.

Table 23: show analytics configuration Command Output Fields (Junos OS Release 13.2X51-D10 and earlier) *(continued)*

Field	Descriptions
Poll interval (traffic statistics)	Interval for traffic statistics polling in seconds. If the output displays a setting of 0 seconds, the polling interval was not configured, and the default interval applies. NOTE: The default interval is 1 second in Junos OS Release 13.2X50-D15 and later, except for EX4300 switches, on which the default interval is 5 seconds, and 2 seconds in Junos OS Release 13.2X51-D10. NOTE: Due to limitations and variations in hardware capability in different devices, there might be a difference in value between the actual interval and configured interval.
Queue statistics	Settings are Auto, Enabled, or Disabled. If **Auto** is displayed, queue statistics monitoring is not enabled.
Poll interval (queue statistics)	Interval for queue statistics polling in milliseconds. NOTE: The default interval is 8 milliseconds in Junos OS Release 13.2X50-D15 and later, and 10 milliseconds in Junos OS Release 13.2X51-D10 or later. NOTE: Due to limitations and variations in hardware capability in different devices, there might be a difference in value between the actual interval and configured interval.
Depth threshold high	Upper limit of the depth threshold configuration in number of bytes. If **0** is displayed, depth threshold is not enabled.
Depth threshold low	Lower limit of the depth threshold configuration in number of bytes. If **0** is displayed, depth threshold is not enabled.
Latency threshold high	Upper limit of the latency threshold configuration in microseconds. If **0** is displayed, latency threshold is not enabled.
Latency threshold low	Lower limit of the latency threshold configuration in microseconds. If **0** is displayed, latency threshold is not enabled.
Interface Configurations	
Interface	Name of interface that is configured for network analytics. The interface configuration overrides the global network analytics configuration.
Traffic Statistics	Settings are Enabled or Disabled for the interface.
Queue Statistics	Settings are Enabled or Disabled for the interface.
Depth-threshold High	Upper limit of the depth threshold configuration in number of bytes. If **0** is displayed, depth threshold is not enabled.

Copyright © 2018, Juniper Networks, Inc.

Table 23: show analytics configuration Command Output Fields (Junos OS Release 13.2X51-D10 and earlier) *(continued)*

Field	Descriptions
Depth-threshold Low	Lower limit of the depth threshold configuration in number of bytes. If **0** is displayed, depth threshold is not enabled.
Latency-threshold High	Upper limit of the latency threshold configuration in microseconds. If **0** is displayed, latency threshold is not enabled.
Latency-threshold Low	Lower limit of the latency threshold configuration in microseconds. If **0** is displayed, latency threshold is not enabled.

Sample Output

show analytics configuration (Junos OS Release 13.2X51-D15 and Later)

```
user@host> show analytics configuration
Traffic monitoring status is enabled
Traffic monitoring polling interval : 5 seconds
Queue monitoring status is enabled
Queue monitoring polling interval : 1000 milliseconds
Queue depth high threshold : 99999 bytes
Queue depth low threshold : 99 bytes

Interface     Traffic       Queue        Queue depth              Latency
            Statistics    Statistics      threshold              threshold
                                         High         Low      High      Low
                                            (bytes)             (nanoseconds)
xe-0/0/16   enabled       enabled        n/a          n/a      2300      20
xe-0/0/18   enabled       enabled        n/a          n/a      2300      20
xe-0/0/19   enabled       enabled        n/a          n/a      2300      20
```

show analytics configuration (Junos OS Release 13.2X51-D10 and Earlier)

```
user@host> show analytics configuration
Global configurations:
   Traffic statistics: Enabled, Poll interval: 2 seconds
   Queue statistics: Auto, Poll interval: 10 milliseconds
   Depth threshold high: 0 bytes, low: 0 bytes
   Latency threshold high: 0 microseconds, low: 0 microseconds
Interface     Traffic       Queue        Depth-threshold      Latency-threshold
            Statistics    Statistics      High      Low        High      Low
                                             (bytes)           (microseconds)
xe-0/0/0     Auto          Auto           204800    10         0         0
```


Copyright © 2018, Juniper Networks, Inc.

show analytics queue-statistics

Syntax

show analytics queue-statistics
<interface *interface-name*>

Release Information

Command introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

Show the queue statistics (queue length and latency) that are collected for all interfaces that are enabled for network analytics on a device. Optionally, if you wish to see the queue statistics for one interface only, you may specify the interface.

Options

interface *interface-name*—(Optional) Display the queue statistics for the specified interface only.

Required Privilege Level

interface-control

Related Documentation

- Network Analytics Overview on page 103
- analytics on page 138

List of Sample Output

show analytics queue-statistics (Junos OS Release 13.2X51-D15 and Later) on page 165
show analytics queue-statistics (Junos OS Release 13.2X51-D10) on page 166
show analytics queue-statistics (Junos OS Release 13.2X50-D15) on page 166

Output Fields

Table 18 on page 121 describes the output fields for the **show analytics queue-statistics** command.

Table 24: show analytics queue-statistics Command Output Fields

Field	Description
Time	Date and time at which the queue statistics are collected.
Interface	Name of the interface at which the queue statistics are collected.
Queue-length or queue-depth (bytes)	Queue depth (length) in number of bytes.
Latency	Queue depth in nanoseconds (Junos OS Release 13.2X51-D15 and later) or microseconds (Junos OS Release 13.2X51-D10 and earlier).

Sample Output

show analytics queue-statistics (Junos OS Release 13.2X51-D15 and Later)

```
user@host> show analytics queue-statistics
```

```
CLI issued at 2014-01-07 17:20:29.978561
Time                        Interface        Queue-depth        Latency
                                             (bytes)            (nanoseconds)
00:00:00.870058 ago         xe-0/0/19        1369680            1095744
00:00:01.875049 ago         xe-0/0/19        1381952            1105561
00:00:02.875053 ago         xe-0/0/19        1387776            1110220
00:00:03.876047 ago         xe-0/0/19        1387568            1110054
00:00:04.873045 ago         xe-0/0/19        1388192            1110553
00:00:05.871044 ago         xe-0/0/19        1385904            1108723
00:00:06.873354 ago         xe-0/0/19        1371552            1097241
```

show analytics queue-statistics (Junos OS Release 13.2X51-D10)

```
user@host> show analytics queue-statistics
Time                    Interface   Queue-length (bytes)   Latency (us)
2013 Nov 3 3:52:26.272 xe-0/0/9        208                   0
2013 Nov 3 3:52:26.292 xe-0/0/9        208                   0
2013 Nov 3 3:52:26.372 xe-0/0/9        208                   0
2013 Nov 3 3:52:26.392 xe-0/0/9        208                   0
2013 Nov 3 3:52:26.432 xe-0/0/9        208                   0
2013 Nov 3 3:52:26.492 xe-0/0/9        208                   0
2013 Nov 3 3:52:26.572 xe-0/0/9        208                   0
2013 Nov 3 4:30:24.584 xe-0/0/9    1387152                1109
2013 Nov 3 4:30:24.604 xe-0/0/9    1372384                1097
2013 Nov 3 4:30:24.624 xe-0/0/9    1384864                1107
```

Sample Output

show analytics queue-statistics (Junos OS Release 13.2X50-D15)

```
user@host> show analytics queue-statistics
Time               Interface   Queue-length (bytes)   Latency (us)
Apr 6 0:17:18.224  xe-0/0/9            1043952            835
Apr 6 0:17:18.234  xe-0/0/9            1053520            842
Apr 6 0:17:18.244  xe-0/0/9            1055184            844
```


Copyright © 2018, Juniper Networks, Inc.

show analytics status

Syntax

show analytics status
<global>

Release Information

Command introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

Show the status of the network analytics components that are configured on a device.

Options

none—Show the global and interface status for network analytics.

global—Show the global status only for network analytics.

NOTE: The **global** option is not available in Junos OS Releases prior to 13.2X51-D15.

Required Privilege Level

interface-control

Related Documentation

- Network Analytics Overview on page 103
- analytics on page 138

List of Sample Output

show analytics status (Junos OS Release 13.2X51-D15 or Later) on page 169
show analytics status global (Junos OS Release 13.2X51-D15 or Later) on page 169
show analytics status (Junos OS Release 13.2X50-D15 and 13.2X51-D10) on page 170

Output Fields

Table 25 on page 167 describes the output fields for the **show analytics status** command.

Table 25: show analytics status Command Output Fields

Field	Descriptions
Global Configurations	
Traffic statistics or Traffic monitoring status	Settings are Auto, Enabled, or Disabled. If **Auto** is displayed, traffic statistics monitoring is not enabled. NOTE: The Disabled setting always supersedes the Enabled setting.
Poll interval or Traffic monitoring polling interval	Interval for traffic statistics polling in seconds. NOTE: Due to limitations and variations in the hardware capability of different devices, you might see a difference in value between the actual interval and configured interval.

Table 25: show analytics status Command Output Fields *(continued)*

Field	Descriptions
Queue statistics or Queue monitoring status	Can be Auto, Enabled, or Disabled. If **Auto** is displayed, queue statistics monitoring is not enabled. NOTE: The Disabled setting always supersedes the Enabled setting.
Poll interval or Queue monitoring polling interval	Interval for queue statistics polling in milliseconds. NOTE: Due to limitations and variations in the hardware capability of different devices, you might see a difference in value between the actual interval and configured interval.
Depth threshold high or Queue depth high threshold	Upper limit of the depth threshold configuration in number of bytes. In Junos OS Release 13.2X51-D15 or later, if this parameter is not configured, this field is not shown. In Junos OS Release 13.2X51-D10 or earlier, if this parameter is not configured, a value of **0** is displayed.
Depth threshold low or Queue depth low threshold	Lower limit of the depth threshold configuration in number of bytes. In Junos OS Release 13.2X51-D15 or later, if this parameter is not configured, this field is not shown. In Junos OS Release 13.2X51-D10 or earlier, if this parameter is not configured, a value of **0** is displayed.
Latency threshold high	Upper limit of the latency threshold configuration in microseconds. In Junos OS Release 13.2X51-D15 or later, if this parameter is not configured, this field is not shown. In Junos OS Release 13.2X51-D10 or earlier, if this parameter is not configured, a value of **0** is displayed.
Latency threshold low	Lower limit of the latency threshold configuration in microseconds. In Junos OS Release 13.2X51-D15 or later, if this parameter is not configured, this field is not shown. In Junos OS Release 13.2X51-D10 or earlier, if this parameter is not configured, a value of **0** is displayed.
Interface Configurations	
Interface	Name of an interface that is configured for network analytics. The interface configuration overrides the global network analytics configuration.
Traffic Statistics	Settings are Enabled or Disabled for the interface. NOTE: The Disabled setting always supersedes the Enabled setting.
Queue Statistics	Settings are Enabled or Disabled for the interface. NOTE: The Disabled setting always supersedes the Enabled setting.

Copyright © 2018, Juniper Networks, Inc.

Table 25: show analytics status Command Output Fields *(continued)*

Field	Descriptions
Depth-threshold High or Queue depth threshold high	Upper limit of the depth threshold configuration in number of bytes. If this parameter is not configured, an output of **n/a** or **0** is displayed in this column, depending on the software release.
Depth-threshold Low or Queue depth threshold low	Lower limit of the depth threshold configuration in number of bytes. If this parameter is not configured, an output of **n/a** or **0** is displayed in this column, depending on the software release.
Latency-threshold High	Upper limit of the latency threshold configuration in nanoseconds or microseconds. If this parameter is not configured, an output of **n/a** or **0** is displayed in this column, depending on the software release.
Latency-threshold Low	Lower limit of the latency threshold configuration in nanoseconds or microseconds. If this parameter is not configured, an output of **n/a** or **0** is displayed in this column, depending on the software release.

Sample Output

show analytics status (Junos OS Release 13.2X51-D15 or Later)

```
user@host> show analytics status
Traffic monitoring status is auto
Traffic monitoring polling interval : 5 seconds
Queue monitoring status is enabled
Queue monitoring status polling interval : 1000 milliseconds
Queue depth high threshold : 1000000000 bytes
Queue depth low threshold : 99 bytes

Interface     Traffic       Queue        Queue depth            Latency
            Statistics    Statistics      threshold             threshold
                                        High        Low         High      Low
                                          (bytes)             (nanoseconds)
xe-0/0/16     enabled     enabled       1000000000  99         n/a       n/a
xe-0/0/18     disabled    enabled       1000000000  99         n/a       n/a
xe-0/0/19     enabled     enabled       1000000000  99         n/a       n/a
```

show analytics status global (Junos OS Release 13.2X51-D15 or Later)

```
user@host> show analytics status global

Traffic monitoring status is auto
Traffic monitoring polling interval : 5 seconds
Queue monitoring status is enabled
Queue monitoring status polling interval : 1000 milliseconds
Queue depth high threshold : 1000000000 bytes
Queue depth low threshold : 99 bytes
```

show analytics status (Junos OS Release 13.2X50-D15 and 13.2X51-D10)

```
user@host> show analytics status
Global configurations:
   Traffic statistics: Auto, Poll interval: 2 seconds
   Queue statistics: Auto, Poll interval: 10 milliseconds
   Depth threshold high: 0 bytes, low: 0 bytes
   Latency threshold high: 1000 microseconds, low: 50 microseconds
Interface     Traffic       Queue        Depth-threshold      Latency-threshold
            Statistics    Statistics      High      Low         High      Low
                                             (bytes)            (microseconds)
xe-0/0/6     Enabled       Enabled       0          0           1000       50
xe-0/0/7     Enabled       Enabled       204800     10          0          0
xe-0/0/8     Enabled       Enabled       0          0           1000       50
```


Copyright © 2018, Juniper Networks, Inc.

show analytics streaming-servers

Syntax show analytics streaming-servers

Release Information Command introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description Show the list of streaming servers that are configured for network analytics. Streaming servers receive streaming output for queue statistics and traffic statistics from the network analytics process (Analyticsd) running on the Routing Engine.

NOTE: **The show analytics streaming-servers command is available in Junos OS Release 13.2X50-D15 and 13.2X51-D10 only.**

Required Privilege Level interface-control

Related Documentation

- Network Analytics Overview on page 103
- analytics on page 138
- show analytics collector on page 159

List of Sample Output show analytics streaming-servers on page 172

Output Fields Table 26 on page 171 describes the output fields for the **show analytics streaming-servers** command.

Table 26: show analytics streaming-servers Command Output Fields

Field	Description
Address	IP Address of the streaming server that is configured for receiving the streaming data.
Port	Port number of the streaming server receiving the streaming data.
Stream-Format	Format of the data that is sent to the server. Values are: • csv—Comma-separated values. • json—JavaScript Object Notification. • tsv—Tab-separated values.
Stream-Type	Type of data that is sent to the a port on the streaming server: • QS—Queue statistics. • TS—Traffic statistics.

Table 26: show analytics streaming-servers Command Output Fields *(continued)*

Field	Description
State	Connection state of the streaming server.
Sent	Number of bytes sent to the streaming server.

Sample Output

show analytics streaming-servers

```
user@host> show analytics streaming-servers
Address        Port     Stream-Format    Stream-Type   State         Sent
10.94.198.14   50001    json             QS            Established   0
10.94.198.14   50005    csv              TS            Established   1185
172.17.28.28   50005    tsv              TS/QS         In Progress   0
```


Copyright © 2018, Juniper Networks, Inc.

show analytics traffic-statistics

Syntax

show analytics traffic-statistics
<interface *interface-name*>

Release Information

Command introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 13.2X51-D25 for EX Series switches.

Description

Show the traffic statistics that are collected for all interfaces that are enabled for network analytics on a device. Optionally, if you wish to see the traffic statistics for one interface only, you may specify the interface.

Options

interface *interface-name*—(Optional) Display the traffic statistics for the specified interface only.

Required Privilege Level

interface-control

Related Documentation

- Network Analytics Overview on page 103
- analytics on page 138

List of Sample Output

show analytics traffic-statistics (Junos OS Release 13.2X51-D15 or Later) on page 174
show analytics traffic-statistics (Junos OS Release 13.2X51-D10) on page 174
show analytics traffic-statistics (Junos OS Release 13.2X50-D15) on page 174

Output Fields

Table 27 on page 173 describes the output fields for the **show analytics traffic-statistics** command.

Table 27: show analytics traffic-statistics Command Output Fields

Field	Description
Time	The date and time at which the traffic statistics are generated.
Physical interface	Name of the interface at which the traffic statistics are collected.
Total octets	Total number of octets that are received and transmitted.
Total packets	Total number of packets that are received and transmitted.
Octets per second	Number of octets received and transmitted per second.
Packet per second	Number of packets received and transmitted per second.

Copyright © 2018, Juniper Networks, Inc.

Table 27: show analytics traffic-statistics Command Output Fields *(continued)*

Field	Description
CRC/Align errors or Octets dropped	Number of cyclic redundancy check (CRC) errors or octets dropped. • Junos OS Release 13.2X51-D15 or later—Number of cyclic redundancy check (CRC) errors. • Junos OS Release 13.2X51-D10 and earlier—Number of octets dropped.
Packets dropped	Number of packets dropped.

Sample Output

show analytics traffic-statistics (Junos OS Release 13.2X51-D15 or Later)

```
user@host> show analytics traffic-statistics
CLI issued at 2014-01-07 17:22:28.952677
Time: 00:00:03.480244 ago, Physical interface: xe-0/0/19
  Traffic Statistics:                Receive               Transmit
  Total octets:                3929946593792        393001011519232
  Total packets:                 30702707784          3070320402462
  Unicast packet:                30702707784          3070320402462
  Multicast packets:                       0                      0
  Broadcast packets:                       0                      0
  Octets per second:                86407016               59044064
  Packets per second:                  84787                8469688
  CRC/Align errors:                        0        392986110751744
  Packets dropped:                         0          3070203990248
```

show analytics traffic-statistics (Junos OS Release 13.2X51-D10)

```
user@host> show analytics traffic-statistics
Time: 2013 Nov 3 4:36:55.542, Physical interface: xe-0/0/8
  Traffic Statistics:                Receive            Transmit
  Total octets:                2777524779008        101855533467
  Total packet:                  21699412289           795746503
  Octets per second:               904001272                   0
  Packet per second:                 8399574                   0
  Octets dropped:                          0                   0
  Packet dropped:                          0                   0
Time: 2013 Nov 3 4:36:57.559, Physical interface: xe-0/0/10
  Traffic Statistics:                Receive            Transmit
  Total octets:                2777546444381        129840936198
  Total packet:                  21699581650          1014382311
  Octets per second:                90400211            86403728
  Packet per second:                 8400382               84438
  Octets dropped:                          0                   0
  Packet dropped:                          0                   0
```

show analytics traffic-statistics (Junos OS Release 13.2X50-D15)

```
user@host> show analytics traffic-statistics
Time: Apr 5 19:52:48.549, Physical interface: xe-0/0/8
  Traffic Statistics:                Receive            Transmit
  Total octets:                4797548752936        408886273632
  Total packet:                   5658257464          3190613435
  Octets per second:                       0                   0
  Packet per second:                       0                   0
```


Copyright © 2018, Juniper Networks, Inc.

```
  Octets dropped:                          0           252901000
  Packet dropped:                          0              252901
  Utilization:                          0.0%                0.0%
Time: Apr 5 19:52:48.549, Physical interface: xe-0/0/10
  Traffic Statistics:                Receive            Transmit
  Total octets:               4790866253100           477139024
  Total packet:                  5624473639              477944
  Octets per second:                       0                   0
  Packet per second:                       0                   0
  Octets dropped:                          0           166582000
  Packet dropped:                          0              166582
  Utilization:                          0.0%                0.0%
```

Copyright © 2018, Juniper Networks, Inc.

PART 4

sFlow Technology

- Configuring sFlow Technology on page 179
- sFlow Technology Configuration Statements on page 191
- sFlow Technology Operational Commands on page 201

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 10

Configuring sFlow Technology

- Understanding How to Use sFlow Technology for Network Monitoring on a Switch on page 179
- Configuring sFlow Technology on page 184
- Example: Monitoring Network Traffic Using sFlow Technology on page 185

Understanding How to Use sFlow Technology for Network Monitoring on a Switch

The sFlow technology is a monitoring technology for high-speed switched or routed networks. sFlow monitoring technology randomly samples network packets and sends the samples to a monitoring station called a *collector*. You can configure sFlow technology on a Juniper Networks switch to continuously monitor traffic at wire speed on all interfaces simultaneously.

This topic describes:

- Sampling Mechanism and Architecture of sFlow Technology on Switches on page 179
- Adaptive Sampling on page 181
- sFlow Agent Address Assignment on page 182
- sFlow Limitations on Switches on page 182

Sampling Mechanism and Architecture of sFlow Technology on Switches

sFlow technology uses the following two sampling mechanisms:

- Packet-based sampling—Samples one packet out of a specified number of packets from an interface enabled for sFlow technology. Only the first 128 bytes of each packet are sent to the collector. Data collected include the Ethernet, IP, and TCP headers, along with other application-level headers (if present). Although this type of sampling might not capture infrequent packet flows, the majority of flows are reported over time, allowing the collector to generate a reasonably accurate representation of network activity. To configure packet-based sampling, you must specify a sample rate.
- Time-based sampling—Samples interface statistics at a specified interval from an interface enabled for sFlow technology. Statistics such as Ethernet interface errors are captured. To configure time-based sampling, you must specify a polling interval.

Copyright © 2018, Juniper Networks, Inc.

The sampling information is used to create a network traffic visibility picture. The Juniper Networks Junos operating system (Junos OS) fully supports the sFlow standard described in RFC 3176, *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks* (see http://faqs.org/rfcs/rfc3176.html).

NOTE: sFlow technology on the switches samples only raw packet headers. A raw Ethernet packet is the complete Layer 2 network frame.

An sFlow monitoring system consists of an sFlow agent embedded in the switch and a centralized collector. The sFlow agent's two main activities are random sampling and statistics gathering. It combines interface counters and flow samples and sends them across the network to the sFlow collector as UDP datagrams, directing those datagrams to the IP address and UDP destination port of the collector. Each datagram contains the following information:

- The IP address of the sFlow agent
- The number of samples
- The interface through which the packets entered the agent
- The interface through which the packets exited the agent
- The source and destination interface for the packets
- The source and destination VLAN for the packets

EX Series switches, QFX Series switches, and the QFabric systems adopt the distributed sFlow architecture. The sFlow agent has two separate sampling entities that are associated with each Packet Forwarding Engine in case of switches and nodes in case of a QFabric system. These sampling entities are known as subagents. Each subagent has a unique ID that is used by the collector to identify the data source. A subagent has its own independent state and forwards its own sample messages to the sFlow agent. The sFlow agent is responsible for packaging the samples into datagrams and sending them to the sFlow collector. Because sampling is distributed across subagents, the protocol overhead associated with sFlow technology is significantly reduced at the collector.

NOTE: On the QFabric system, an sFlow collector must be reachable through the data network. Because each Node device has all routes stored in the default routing instance, the collector IP address should be included in the default routing instance to ensure the collector's reachability from the Node device.

NOTE: You cannot configure sFlow monitoring on a link aggregation group (LAG), but you can configure it individually on a LAG member interface.

Copyright © 2018, Juniper Networks, Inc.

Infrequent sampling flows might not be reported in the sFlow information, but over time the majority of flows are reported. Based on a configured sampling rate *N*, 1 out of *N* packets is captured and sent to the collector. This type of sampling does not provide a 100 percent accurate result in the analysis, but it does provide a result with quantifiable accuracy. A user-configured polling interval defines how often the sFlow data for a specific interface are sent to the collector, but an sFlow agent can also schedule polling.

NOTE: We recommend that you configure the same sample rate for all the ports in a line card. If you configure different sample rates, the lowest value is used for all ports on the line card..

NOTE: If the mastership assignment changes in a Virtual Chassis setup, sFlow technology continues to function.

Adaptive Sampling

To ensure sampling accuracy and efficiency, EX Series switches and QFX Series devices use adaptive sFlow sampling. Adaptive sampling monitors the overall incoming traffic rate on the device and provides feedback to the interfaces to dynamically adapt their sampling rate to traffic conditions. The sFlow agent reads the statistics on the interfaces every few seconds (12 seconds for EX Series switches and 5 seconds for QFX Series devices) and identifies five interfaces with the highest number of samples.

On a Flexible PIC Concentrator (FPC), when the CPU processing limit is reached because of sflow sample processing, a binary backoff algorithm is initiated. This reduces the sampling load, arriving through the top five sample-producing interfaces on that FPC by half. The backoff algorithm achieves this by doubling the sampling rate on these five earmarked interfaces. This process is repeated until the CPU-load due to sflow on the given FPC comes down to an acceptable level.

On a QFabric system, sFlow technology monitors the interfaces on each node device as a group, and implements the binary backoff algorithm based on the traffic on that group of interfaces.

NOTE: On the QFX Series standalone switches, if you configure sFlow technology monitoring on multiple interfaces and with a high sampling rate, we recommend that you specify a collector that is on the data network instead of on the management network. Having a high volume of sFlow technology monitoring traffic on the management network might interfere with other management interface traffic.

Using adaptive sampling prevents overloading of the CPU and keeps the device operating at its optimum level even when there is a change in traffic patterns on the interfaces. The reduced sampling rate is used until the device is rebooted or when a new sampling rate is configured.

Copyright © 2018, Juniper Networks, Inc.

NOTE: sFlow technology on EX Series switches does not support graceful restart. When a graceful restart occurs, the adaptive sampling rate is set to the user-configured sampling rate.

sFlow Agent Address Assignment

The sFlow collector uses the sFlow agent's IP address to determine the source of the sFlow data. You can configure the IP address of the sFlow agent to ensure that the agent ID of the sFlow agent remains constant. If you do not specify the IP address to be assigned to the agent, an IP address is automatically assigned to the agent based on the following order of priority of interfaces configured on the device:

EX Series Devices	QFX Series Devices
1. Virtual Management Ethernet (VME) interface 2. Management Ethernet interface	1. Management Ethernet interface me0 IP address 2. Any Layer 3 interface if the me0 IP address is not available

If a particular interface is not configured, the IP address of the next interface in the priority list is used as the IP address for the agent. Once an IP address is assigned to the agent, the agent ID is not modified until the sFlow service is restarted. At least one interface has to be configured for an IP address to be assigned to the agent. When the agent's IP address is assigned automatically, the IP address is dynamic and changes when the switch reboots.

On the QFabric system, the following default values are used if the optional parameters are not configured:

- Agent ID is the management IP address of the default partition.
- Source IP is the management IP address of the default partition.

In addition, the QFabric system subagent ID (which is included in the sFlow datagrams) is the ID of the node group from which the datagram is sent to the collector.

sFlow data can be used to provide network traffic visibility information. You can explicitly configure the source IP address to be assigned to the sFlow datagrams. If you do not explicitly configure the IP address, the IP address of any of the configured Layer 3 network interfaces is used as the source IP address. If a Layer 3 IP address is not configured, then the agent IP address is used as the source IP address.

sFlow Limitations on Switches

On the QFX Series, limitations of sFlow traffic sampling include the following:

- sFlow sampling on ingress interfaces does not capture CPU-bound traffic.
- sFlow sampling on egress interfaces does not support broadcast and multicast packets.
- Egress samples do not contain modifications made to the packet in the egress pipeline.

Copyright © 2018, Juniper Networks, Inc.

- If a packet is discarded because of a firewall filter, the reason code for discarding the packet is not sent to the collector.
- The out-priority field for a VLAN is always set to 0 (zero) on ingress and egress samples.
- On QFX5100 standalone switches and the QFX Series Virtual Chassis (including mixed QFX Series Virtual Chassis), egress firewall filters are not applied to sFlow sampling packets. On these platforms, the software architecture is different from that on other QFX Series devices—sFlow packets are sent by the Routing Engine (not the line card on the host) and do not transit the switch. Egress firewall filters affect data packets that are transiting a switch, but do not affect packets sent by the Routing Engine. As a result, sFlow sampling packets are always sent to the sFlow collector.

EX9200 switches support configuration of only one sampling rate (inclusive of ingress and egress rates) on an FPC. To support compatibility with the sflow configuration of other Juniper Networks products, EX9200 switches still accept multiple rate configuration on different interfaces of the same FPC. However, the switch programs the lowest rate as the sampling rate for all the interfaces of that FPC. The sFlow show command (**show sflow interfaces**) displays the configured rate and the actual (effective) rate. However, different rates on different FPCs is still supported on EX9200 switches.

Related Documentation

- Example: Monitoring Network Traffic Using sFlow Technology on page 185
- *Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches*
- Configuring sFlow Technology on page 184
- *Configuring sFlow Technology for Network Monitoring (CLI Procedure)*
- *Monitoring Interface Status and Traffic*

Configuring sFlow Technology

The sFlow technology is a monitoring technology for high-speed switched or routed networks. sFlow monitoring technology collects samples of network packets and sends them in a UDP datagram to a monitoring station called a *collector*. You can configure sFlow technology on a device to monitor traffic continuously at wire speed on all interfaces simultaneously. You must enable sFlow monitoring on each interface individually; you cannot globally enable sFlow monitoring on all interfaces with a single configuration statement. Junos OS supports the sFlow technology standard described in RFC 3176, *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*.

On the QFabric system, the sFlow monitoring global configuration that is defined on the Director device is distributed to Node groups that have sFlow sampling configured on the interfaces.

To configure sFlow features using the CLI:

1. Configure the IP address and UDP port of at least one collector:

   ```
   [edit protocols sflow]
   user@host# set collector ip-address udp-port port-number
   ```

   The default UDP port assigned is 6343.

2. Enable sFlow technology on a specific interface:

   ```
   [edit protocols sflow]
   user@host# set interfaces interface-name
   ```

   NOTE: You cannot enable sFlow technology on a LAG interface (for example ae0), but you can enable sFlow technology on the member interfaces of the LAG (for example, xe-0/0/1).

3. Specify how often (in seconds) the sFlow agent polls all interfaces at the global level:

   ```
   [edit protocols sflow]
   user@host# set polling-interval seconds
   ```

   NOTE: Specify 0 if you do not want to poll the interface.

4. Specify the rate at which packets are sampled at the global level. For example, configuring a ***number*** of 1000 sets a sample rate of 1 in 1000 packets.

   ```
   [edit protocols sflow]
   user@host# set sample-rate number
   ```


Copyright © 2018, Juniper Networks, Inc.

NOTE: On QFX10000 Series switches, the hardware might generate more samples that it can handle under heavy traffic loads. The extra samples are dropped by the software and can cause inaccurate results. You can use the *disable-sw-rate-limiter* configuration statement so that the hardware sampling rate stays within the maximum sampling rate of 1 out of 65,536 packets.

5. (Optional) You can also configure the polling interval and sample rate at the interface level:

```
[edit protocols sflow]
user@host# set interfaces interface-name polling-interval seconds sample-rate number
```

NOTE: The interface-level configuration overrides the global configuration for the specified interface.

Related Documentation

- *Overview of sFlow Technology*
- Example: Monitoring Network Traffic Using sFlow Technology on page 185
- *disable-sw-rate-limiter*

Example: Monitoring Network Traffic Using sFlow Technology

The sFlow technology is a monitoring technology for high-speed switched or routed networks. sFlow monitoring technology collects samples of network packets and sends them in a UDP datagram to a monitoring station called a *collector*. You can configure sFlow technology on a device to monitor traffic continuously at wire speed on all interfaces simultaneously. You must enable sFlow monitoring on each interface individually; you cannot globally enable sFlow monitoring on all interfaces with a single configuration statement. Junos OS supports the sFlow technology standard described in RFC 3176, *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*.

This example describes how to configure and use sFlow monitoring on a QFX3500 switch in standalone mode.

- Requirements on page 186
- Overview on page 186
- Configuration on page 187
- Verification on page 188

Requirements

This example uses the following hardware and software components:

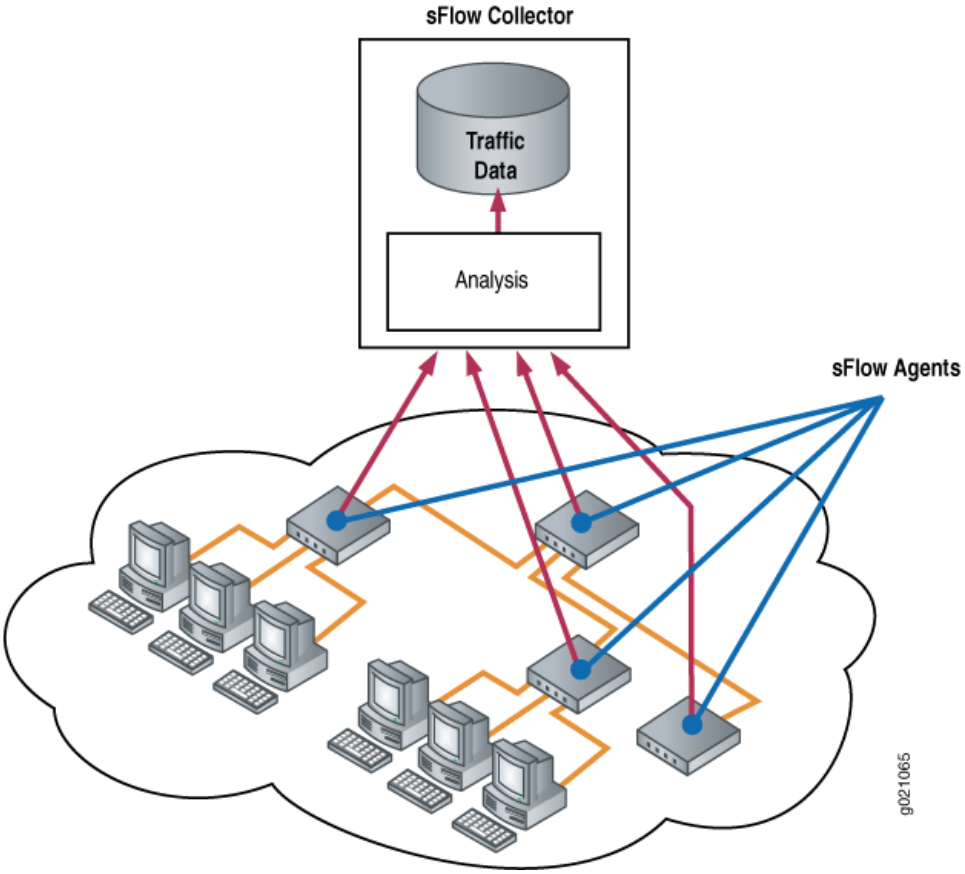
- Junos OS Release 11.3 or later
- One QFX3500 switch

Overview

An sFlow monitoring system consists of an sFlow agent embedded in the device and a centralized collector on the network. The two main activities of the sFlow agent are random sampling and statistics gathering. The sFlow agent combines interface counters and flow samples and sends them to the IP address and UDP destination port of the sFlow collector in UDP datagrams.

Figure 4 on page 186 depicts the basic elements of an sFlow system.

Figure 4: sFlow Technology Monitoring System



Copyright © 2018, Juniper Networks, Inc.

Configuration

CLI Quick Configuration

To quickly configure sFlow technology, copy the following commands and paste them into the terminal window of the switch:

```
[edit protocols sflow]
set collector 10.204.32.46 udp-port 5600
set interfaces xe-0/0/1.0
set polling-interval 20
set sample-rate 1000
```

Step-by-Step Procedure

To configure sFlow features using the CLI:

1. Configure the IP address and UDP port of at least one collector:

   ```
   [edit protocols sflow]
   user@switch# set collector 10.204.32.46 udp-port 5600
   ```

   The default UDP port assigned is 6343.

2. Enable sFlow technology on a specific interface:

   ```
   [edit protocols sflow]
   user@switch# set interfaces xe-0/0/1.0
   ```

   NOTE: You cannot enable sFlow technology on a Layer 3 VLAN-tagged interface.

   You cannot enable sFlow technology on a LAG interface (for example, ae0), but you can enable sFlow technology on the member interfaces of the LAG (for example, xe-0/0/1).

3. Specify how often (in seconds) the sFlow agent polls all interfaces at the global level:

   ```
   [edit protocols sflow]
   user@switch# set polling-interval 20
   ```

   NOTE: Specify 0 if you do not want to poll the interface.

4. Specify the rate at which packets must be sampled at the global level. The following example sets a sample rate of 1 in 1000 packets:

   ```
   [edit protocols sflow]
   ```

```
user@switch# set sample-rate 1000
```

Results Check the results of the configuration:

```
[edit]
user@switch# show protocols
sflow {
  collector 10.204.32.46 {
    udp-port 5600;
  }
  interfaces xe-0/0/1.0 {
    polling-interval 20;
    sample-rate 1000;
  }
}
```

Verification

To confirm that the configuration is correct, perform these tasks:

- Verifying That sFlow Technology Has Been Configured Properly on page 188
- Verifying That sFlow Technology Is Enabled on an Interface on page 189
- Verifying the sFlow Collector Configuration on page 189

Verifying That sFlow Technology Has Been Configured Properly

Purpose Verify that sFlow technology has been configured properly.

Action Enter the **show sflow** operational mode command:

```
user@switch> show sflow
sFlow            : Enabled
Sample limit     : 300 packets/second
Polling interval : 20 second
Sample rate      : 1:1000
Agent ID         : 10.1.1.2
```

NOTE: **The sample limit cannot be configured and is set to 300 packets per second.**

Meaning The output shows that sFlow technology is enabled and specifies the values for the sampling limit, polling interval, and sampling rate.

Copyright © 2018, Juniper Networks, Inc.

Verifying That sFlow Technology Is Enabled on an Interface

Purpose Verify that sFlow technology is enabled on interfaces and display the sampling parameters.

Action Enter the **show sflow interface** operational mode command:

```
user@switch> show sflow interface
Interface        Status      Sample      Polling
                              rate       interval
xe-0/0/1.0    Enabled       1000          20
```

Meaning The output indicates that sFlow technology is enabled on the **Node1:xe-0/0/1.0** interface on the Node device with a sampling rate of 1000 and a polling interval of 20 seconds.

Verifying the sFlow Collector Configuration

Purpose Verify the sFlow collector configuration.

Action Enter the **show sflow collector** operational mode command:

```
user@switch> show sflow collector
Collector         Udp-port    No. of samples
 address
10.204.32.46          5600           7516
```

Meaning The output displays the IP address of the collector, the UDP port, and the number of samples collected.

Related Documentation

- Configuring sFlow Technology on page 184
- *Overview of sFlow Technology*

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 11

sFlow Technology Configuration Statements

- agent-id on page 191
- collector (sFlow Technology) on page 192
- interfaces (sFlow) on page 193
- polling-interval on page 194
- sample-rate on page 195
- sflow on page 196
- source-ip on page 197
- traceoptions (sFlow Technology) on page 198
- udp-port on page 199

agent-id

Syntax agent-id *ip-address*;

Hierarchy Level [edit protocols sflow]

Release Information Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure the IP address of the sFlow agent. If you do not configure the sFlow agent ID, the IP address for the agent is dynamically created using the IP address of an interface configured on the QFX Series device.

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

Related Documentation
- Configuring sFlow Technology on page 184
- **sflow on page 196**

collector (sFlow Technology)

Syntax

```
collector ip-address {
   udp-port port-number;
}
```

Hierarchy Level

[edit protocols sflow]

Release Information

Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Statement introduced in Junos OS Release 17.2R1 for the ACX5000 line of routers.

Description

Configure a remote collector for sFlow network traffic monitoring. The device sends sFlow UDP datagrams to the configured collector for analysis. You can configure up to four collectors on the device. You specify the IP address for each collector you configure.

The remaining statement is explained separately. See CLI Explorer.

Options

ip-address—IP address of the collector.

Required Privilege Level

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

Related Documentation

- Configuring sFlow Technology on page 184
- Example: Monitoring Network Traffic Using sFlow Technology on page 185

Copyright © 2018, Juniper Networks, Inc.

interfaces (sFlow)

Syntax

```
interfaces interface-name {
    polling-interval seconds;
    sample-rate number;
}
```

Hierarchy Level

[edit protocols sflow]

Release Information

Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Statement introduced in Junos OS Release 17.2R1 for the ACX5000 line of routers.

Description

Configure sFlow network traffic monitoring on the specified interface on the device. You can configure sFlow parameters (polling interval, sample rate) with different values on different interfaces.

The remaining statements are explained separately. See CLI Explorer.

Options

interface-name—Name of the interface on which to configure sFlow parameters.

Required Privilege Level

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

Related Documentation

- Configuring sFlow Technology on page 184
- Example: Monitoring Network Traffic Using sFlow Technology on page 185

polling-interval

Syntax polling-interval *seconds*;

Hierarchy Level [edit protocols sflow],
[edit protocols sflow interfaces *interface-name*]

Release Information Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Statement introduced in Junos OS Release 17.2R1 for the ACX5000 line of routers.

Description Configure the rate (in seconds) at which successive samples of interface statistics (counters) are taken.

Default If no polling interval is configured for a particular interface, the device uses the global polling interval configured at the **[edit protocols sflow]** hierarchy level. If no global interval is configured, the device uses the default polling interval of 20 seconds.

Options ***seconds***—Number of seconds between successive samples of interface statistics. Specifying a value of **0** (zero) disables the polling.

Range: 0 through 3600 seconds

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

Related Documentation

- Configuring sFlow Technology on page 184
- Example: Monitoring Network Traffic Using sFlow Technology on page 185

 Copyright © 2018, Juniper Networks, Inc.

sample-rate

Syntax sample-rate *number*;

Hierarchy Level [edit protocols sflow],
[edit protocols sflow interfaces *interface-name*]

Release Information Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Statement introduced in Junos OS Release 17.2R1 for the ACX5000 line of routers.

Description Specify the denominator (***number***) of the ratio that is the sample rate in sFlow traffic monitoring. For example, to configure a sample rate of 1 in 1000 packets, you specify a ***number*** of 1000.

Default If no sample rate is configured for a particular interface, the device uses the global sample rate configured at the **[edit protocols sflow]** hierarchy level. If no global rate is configured, the device uses the default sample rate of 1 in 2000 packets.

Options ***number***—Denominator of the ratio representing the sample rate (one packet out of ***number***).

Range: 1 through 16,777,215

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

Related Documentation

- Configuring sFlow Technology on page 184
- Example: Monitoring Network Traffic Using sFlow Technology on page 185

sflow

Syntax

```
sflow {
  agent-id ip-address;
  collector ip-address {
    udp-port port-number;
  }
  interfaces interface-name {
    polling-interval number;
    sample-rate {
      egress number;
      ingress number;
    }
  }
  polling-interval number;
  sample-rate {
    ingress number;
    egress number;
  }
  source-ip ip-address;
  disable-sw-rate-limiter;
  }
  traceoptions {
    file filename <files number> <no-stamp> <replace> <size size> <world-readable |
      no-world-readable>;
    flag flag;
  }
}
```

Hierarchy Level

[edit protocols]

Release Information

Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Statement introduced in Junos OS Release 17.2R1 for the ACX5000 line of routers.

Description

Configure sFlow technology to monitor traffic continuously on specified interfaces simultaneously. sFlow data can be used to characterize network activity.

The remaining statements are explained separately. See CLI Explorer.

Default

The sFlow protocol is disabled by default.

Required Privilege Level

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

Related Documentation

- Configuring sFlow Technology on page 184
- Example: Monitoring Network Traffic Using sFlow Technology on page 185

Copyright © 2018, Juniper Networks, Inc.

source-ip

Syntax source-ip *ip-address*;

Hierarchy Level [edit protocols sflow]

Release Information Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure the source IP address to be used for sFlow datagrams. If you do not configure a source IP address, it is dynamically created based on the IP address of an Ethernet interface configured on the QFX Series device.

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

Related Documentation

- Configuring sFlow Technology on page 184
- sflow on page 196

traceoptions (sFlow Technology)

Syntax

```
traceoptions {
  file filename <files number> <no-stamp> <replace> <size size> <world-readable |
    no-world-readable>;
  flag flag;
}
```

Hierarchy Level [edit protocols sflow]

Release Information Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Define tracing operations for sFlow technology.

Default The **traceoptions** feature is disabled.

Options

file *filename*—Name of the file to receive the tracing operation output. Enclose the name in quotation marks. Output files are located in the **/var/log/** directory.

files *number*—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**. Incoming trace file data is logged in the now empty **trace-file**. When **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 the maximum number of files, you must also specify the maximum file size using the **size** option.

Range: 2 through 1000 files

Default: 1 trace file

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements.

- all—Trace all sFlow monitoring events.
- client-server—Trace sFlow monitoring client-server events.
- configuration—Trace sFlow monitoring configuration events.
- interface—Trace sFlow monitoring interface events.
- rtsock—Trace routing socket code events.

no-stamp—(Optional) Do not place timestamp information at the beginning of each line in the trace file.

no-world-readable—(Optional) Prevent any user from reading the trace file.

 Copyright © 2018, Juniper Networks, Inc.

replace—(Optional) Replace an existing trace file if there is one.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**. Incoming trace file data is logged in the now empty **trace-file**. When **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 must also specify a maximum number of trace files with the files option.

Syntax: **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

Range: 10 KB through the maximum file size of 4 GB

Default: 128 KB

world-readable—(Optional) Allow any user to read the trace file.

Required Privilege Level

routing and trace—To view this statement in the configuration.
routing-control and trace-control—To add this statement to the configuration.

Related Documentation

- *Overview of sFlow Technology*

udp-port

Syntax

udp-port *port-number*;

Hierarchy Level

[edit protocols sflow collector]

Release Information

Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Statement introduced in Junos OS Release 17.2R1 for the ACX5000 line of routers.

Description

Configure the UDP port for a remote collector for sFlow network traffic monitoring. The device sends sFlow UDP datagrams to the collector for analysis.

Default

Port 6343

Options

port-number—UDP port number for this collector.

Required Privilege Level

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

Related Documentation

- Configuring sFlow Technology on page 184
- Example: Monitoring Network Traffic Using sFlow Technology on page 185

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 12

sFlow Technology Operational Commands

- clear sflow collector statistics
- show sflow
- show sflow collector
- show sflow interface

Copyright © 2018, Juniper Networks, Inc.

clear sflow collector statistics

Syntax clear sflow collector statistics

Release Information Command introduced in Junos OS Release 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Command introduced in Junos OS Release 17.2R1 for the ACX5000 line of routers.

Description Clear the sample counters for all sFlow collectors.

Required Privilege Level view

Related Documentation

- Example: Monitoring Network Traffic Using sFlow Technology on page 185
- Configuring sFlow Technology on page 184
- show sflow collector on page 205

List of Sample Output clear sflow collector statistics on page 202

Sample Output

clear sflow collector statistics

The following example shows two output examples for the **show sflow collector** command, one before and one after the **clear sflow collector statistics** command was issued.

```
user@host> show sflow collector
Collector        Udp-port    No. of samples
   address
   10.1.1.1            6343        3174
   10.1.2.1            6343        3562

user@host> clear sflow collector statistics

user@host> show sflow collector
Collector        Udp-port    No. of samples
   address
   10.1.1.1             6343        0
   10.1.2.1             6343        0
```

 Copyright © 2018, Juniper Networks, Inc.

show sflow

Syntax

show sflow
<collector>
<interface>

Release Information

Command introduced in Junos OS Release 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Command introduced in Junos OS Release 17.2R1 for the ACX5000 line of routers.

Description

Display sFlow configuration information.

Options

none—Display all sFlow configuration information.

collector—(Optional) Display a list of configured sFlow collectors and their properties.

interface—(Optional) Display the interfaces on which sFlow technology is enabled and the sampling parameters.

Required Privilege Level

view

Related Documentation

- show sflow interface on page 206
- show sflow collector on page 205
- clear sflow collector statistics on page 202
- Example: Monitoring Network Traffic Using sFlow Technology on page 185
- Configuring sFlow Technology on page 184

List of Sample Output

show sflow on page 204

Output Fields

Table 28 on page 203 lists the output fields for the **show sflow** command. Output fields are listed in the approximate order in which they appear.

Table 28: show sflow Output Fields

Field Name	Field Description	Level of Output
sFlow	Status of the feature: **Enabled** or **Disabled**.	All levels
Sample limit	Number of packets sampled per second. This sample limit cannot be configured and is set to 300 packets per second.	All levels
Polling interval	Interval at which the sFlow agent polls the interface.	All levels
Sample rate egress	Rate at which egress packets are sampled.	All levels

Table 28: show sflow Output Fields *(continued)*

Field Name	Field Description	Level of Output
Sample rate ingress	Rate at which ingress packets are sampled.	All levels
Agent ID	IP address assigned to the sFlow agent.	All levels
Source IP address	Source IP address for the sFlow packets.	All levels

Sample Output

show sflow

```
user@host> show sflow

sFlow                    : Enabled
Sample limit             : 300 packets/second
Polling interval         : 20 second
Sample rate egress       : 1:2048: Disabled
Sample rate ingress      : 1:1000: Enabled
Agent ID                 : 10.93.54.7
Source IP address        : 10.93.54.7
```


Copyright © 2018, Juniper Networks, Inc.

show sflow collector

Syntax show sflow collector

Release Information Command introduced in Junos OS Release 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Command introduced in Junos OS Release 17.2R1 for the ACX5000 line of routers.

Description Display a list of configured sFlow collectors and their properties.

Required Privilege Level view

Related Documentation

- clear sflow collector statistics on page 202
- show sflow on page 203
- show sflow interface on page 206
- Example: Monitoring Network Traffic Using sFlow Technology on page 185
- Configuring sFlow Technology on page 184

List of Sample Output show sflow collector on page 205

Output Fields Table 29 on page 205 lists the output fields for the **show sflow collector** command. Output fields are listed in the approximate order in which they appear.

Table 29: show sflow collector Output Fields

Field Name	Field Description	Level of Output
Collector address	IP address of the collector.	All levels
UDP-Port	UDP port number of the collector.	All levels
No. of samples	Number of samples collected.	All levels

Sample Output

show sflow collector

```
user@host> show sflow collector

Collector         Udp-port    No. of samples
 address
10.204.32.46        6343          1000
198.51.100.76     3400       1000
```

show sflow interface

Syntax show sflow interface

Release Information Command introduced in Junos OS Release 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Command introduced in Junos OS Release 17.2R1 for the ACX5000 line of routers.

Description Display the interfaces on which sFlow is enabled and the sampling parameters for the interface.

Required Privilege Level view

Related Documentation

- show sflow on page 203
- show sflow collector on page 205
- Example: Monitoring Network Traffic Using sFlow Technology on page 185
- Configuring sFlow Technology on page 184

List of Sample Output show sflow interface (QFX3500 Switch in Standalone Mode) on page 207
show sflow interface (QFabric System) on page 207

Output Fields Table 30 on page 206 lists the output fields for the **show sflow interface** command. Output fields are listed in the approximate order in which they appear.

Table 30: show sflow interface Output Fields

Field Name	Field Description	Level of Output
Interface	Interface on which sFlow technology is enabled.	All levels
Status Egress	Indicates whether an egress sample rate is enabled.	All levels
Status Ingress	Indicates whether an ingress sample rate is enabled.	All levels
Sample rate Egress	Rate at which egress packets are sampled.	All levels
Sample rate Ingress	Rate at which ingress packets are sampled.	All levels
Adapted sample rate Egress	Adapted rate at which egress packets are sampled.	All levels
Adapted sample rate Ingress	Adapted rate at which ingress packets are sampled.	All levels
Polling-interval	Interval at which the sFlow agent polls the interface.	All levels

 Copyright © 2018, Juniper Networks, Inc.

Sample Output

show sflow interface (QFX3500 Switch in Standalone Mode)

```
user@host> show sflow interface
Interface  Status         Sample rate    Adapted sample rate   Polling-interval
              Egress Ingress   Egress Ingress   Egress Ingress
xe-0/0/0.0    Enabled  Disabled  1000    2048    1000     2048            20
xe-1/0/1.0    Enabled  Disabled  1000    2048    1000     2048            20
```

Sample Output

show sflow interface (QFabric System)

```
user@host> show sflow interface
Interface  Status         Sample rate    Adapted sample rate   Polling-interval
              Egress Ingress   Egress Ingress   Egress Ingress
node1:xe-0/0/0.0    Enabled  Disabled  1000    2048    1000     2048
20
node2:xe-1/0/1.0    Enabled  Disabled  1000    2048    1000     2048
20
node4:xe-1/0/0.0    Enabled  Disabled  1000    2048    1000     2048
20
```

Copyright © 2018, Juniper Networks, Inc.

PART 5

SNMP

- Configuring SNMP on page 211
- SNMP Configuration Statements on page 283
- SNMP Operational Commands on page 385

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 13

Configuring SNMP

- Understanding the Implementation of SNMP on page 212
- Utility MIB on page 214
- SNMPv3 Overview on page 215
- Minimum SNMPv3 Configuration on a Device Running Junos OS on page 216
- Understanding RMON on page 217
- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Understanding Health Monitoring on page 221
- SNMP MIBs Support on page 223
- SNMP Traps Support on page 236
- Juniper Networks Enterprise-Specific MIBs on page 248
- MIB Objects for the QFX Series on page 251
- Configuring SNMP on page 254
- Configuring the SNMP Community String on page 257
- Configuring SNMP Trap Groups on page 258
- Adding a Group of Clients to an SNMP Community on page 259
- Configuring the Interfaces on Which SNMP Requests Can Be Accepted on page 260
- Configuring MIB Views on page 261
- Configuring RMON Alarms and Events on page 262
- Configuring Health Monitoring on page 265
- Creating SNMPv3 Users on page 266
- Configuring Access Privileges for a Group on page 267
- Assigning a Security Name to a Group on page 268
- Configuring SNMPv3 Traps on a Device Running Junos OS on page 269
- Configuring SNMP Informs on page 270
- Monitoring RMON MIB Tables on page 271
- Monitoring SNMP on page 272
- Tracing SNMP Activity on a Device Running Junos OS on page 274

Copyright © 2018, Juniper Networks, Inc.

- Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage on page 277
- Example: Configuring SNMP on page 279

Understanding the Implementation of SNMP

The QFX Series products support the Simple Network Management Protocol (SNMP) that is implemented in the Junos OS software.

NOTE: **By default, SNMP is not enabled on devices running Junos OS. For information on enabling SNMP on a device running Junos OS, see** "Configuring SNMP" on page 254.

A typical SNMP implementation includes the following components:

- Network management system (NMS)—The NMS is a combination of hardware and software that is used to monitor and administer a network. Software running on the NMS includes the SNMP manager, which collects information about network connectivity, activity, and events by polling the managed devices.
- Managed device—A managed device (also called a network element) is any device managed by the NMS. Routers and switches are common examples of managed devices. The SNMP agent is the SNMP process that resides on the managed device and communicates with the NMS.
- SNMP agent—The SNMP agent exchanges network management information with SNMP manager software running on an NMS, or host. The agent responds to requests for information and actions from the manager. The agent also controls access to the agent's MIB, the collection of objects that can be viewed or changed by the SNMP manager.

SNMP data is stored in a highly structured, hierarchical format known as a management information base (MIB). The MIB structure is based on a tree structure, which defines a grouping of objects into related sets. Each object in the MIB is associated with an object identifier (OID), which names the object. The "leaf" in the tree structure is the actual managed object instance, which represents a resource, event, or activity that occurs in your network device. The SNMP implementation in Junos OS uses both standard (developed by IETF and documented in RFCs) and Juniper Networks enterprise-specific MIBs.

Communication between the agent and the manager occurs in one of the following forms:

- **Get**, **GetBulk**, and **GetNext** requests—The manager requests information from the agent; the agent returns the information in a **Get** response message.
- **Set** requests—The manager changes the value of a MIB object controlled by the agent; the agent indicates status in a **Set** response message.
- **Traps** notification—The agent sends traps to notify the manager of significant events that occur on the network device.

 Copyright © 2018, Juniper Networks, Inc.

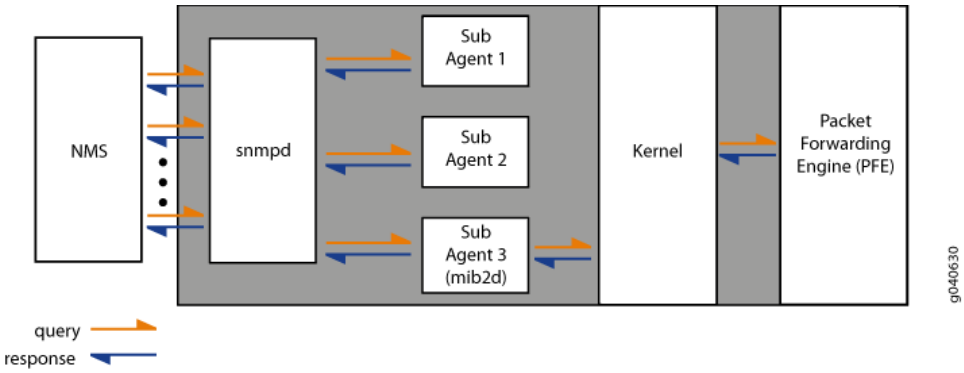
The processes maintaining the SNMP management data include:

- A master SNMP agent (known as SNMP process, or snmpd) that resides on the managed device and is managed by the NMS or host.
- Various subagents that reside on different modules of Junos OS, such as the Routing Engine, and are managed by the master SNMP agent.
- Junos OS processes that share data with the subagents when polled for SNMP data (for example, interface-related MIBs).

When an NMS polls the master agent for data, the master agent immediately shares the data with the NMS if the requested data is available from the master agent or one of the subagents. However, if the requested data is not maintained by the master agent or subagents, the subagent polls the Junos OS kernel or the process that maintains that data. The Junos OS kernel may need to get the data from the Packet Forwarding Engine. On receiving the required data, the subagent passes the response back on to the master agent, which in turn passes it on to the NMS.

Figure 5 on page 213 shows the communication flow among the NMS, SNMP master agent (snmpd), SNMP subagents, Junos OS kernel, and Packet Forwarding Engine.

Figure 5: SNMP Communication Flow



When a significant event, most often an error or a failure, occurs on a network device, the SNMP agent sends notifications to the SNMP manager. SNMP notifications can be sent as traps (unconfirmed notifications) or inform requests (confirmed notifications).

Junos OS supports trap queuing to ensure that traps are not lost because of temporary unavailability of routes. Two types of queues, destination queues and a throttle queue, are formed to ensure delivery of traps and control the trap traffic. On QFX Series products, the maximum size of trap queues (throttle queue plus destination queue) is 40,960 traps. The maximum size of any one queue is 20,480 traps.

Junos OS forms a destination queue when a trap to a particular destination is returned because the host is not reachable, and it adds the subsequent traps to the same destination to the queue. Junos OS checks for availability of routes every 30 seconds, and sends the traps from the destination queue in a round-robin fashion.

If the trap delivery fails, the trap is added back to the queue, and the delivery attempt counter and the next delivery attempt timer for the queue are reset. Subsequent attempts

Copyright © 2018, Juniper Networks, Inc.

occur at progressive intervals of 1 minute, 2 minutes, 4 minutes, and 8 minutes. The maximum delay between the attempts is 8 minutes, and the maximum number of attempts is ten. After ten unsuccessful attempts, the destination queue and all the traps in the queue are deleted.

Junos OS also has a throttle mechanism to control the number of traps (throttle threshold) sent during a particular time period (throttle interval). The throttle mechanism ensures consistency in trap traffic, especially when large numbers of traps are generated because of interface status changes. The throttle interval period begins when the first trap arrives at the throttle. All traps within the trap threshold are processed, and the traps beyond the threshold limit are queued. The default throttle threshold is 500 traps, and the throttle interval default is 5 seconds.

NOTE: **You cannot configure trap queueing in Junos OS. You cannot view information about trap queues except for what is provided in the system logs.**

Related Documentation

- Configuring SNMP on page 254
- SNMP MIBs Support on page 223
- SNMP Traps Support on page 236

Utility MIB

The Juniper Networks enterprise-specific Utility MIB, whose object ID is {jnxUtilMibRoot 1}, defines objects for counters, integers, and strings. The Utility MIB contains one table for each of the following five data types:

- 32-bit counters
- 64-bit counters
- Signed integers
- Unsigned integers
- Octet strings

Each data type has an arbitrary ASCII name, which is defined when the data is populated, and a timestamp that shows the last time when the data instance was modified. For a downloadable version of this MIB, see *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide*.

For information about the enterprise-specific Utility MIB objects, see the following topics:

- *jnxUtilCounter32Table*
- *jnxUtilCounter64Table*
- *jnxUtilIntegerTable*

 Copyright © 2018, Juniper Networks, Inc.

- *jnxUtilUintTable*
- *jnxUtilStringTable*

Related Documentation

- *Enterprise-Specific SNMP MIBs Supported by Junos OS*
- *Standard SNMP MIBs Supported by Junos OS*
- *Understanding the Implementation of SNMP on the QFabric System*

SNMPv3 Overview

The QFX3500 switch supports SNMP version 3 (SNMPv3). SNMPv3 enhances the functionality of SNMPv1 and SNMPv2c by supporting user authentication and data encryption. SNMPv3 uses the user-based security model (USM) to provide security for SNMP messages, and the view-based access control model (VACM) for user access control.

SNMPv3 features include:

- With USM, the SNMP messages between the SNMP manager and the agent can have the message source authenticated and the data integrity checked. USM reduces messaging delays and message replays by enforcing timeout limits and by checking for duplicate message request IDs.
- VACM complements USM by providing user access control for SNMP queries to the agent. You define access privileges that you wish to extend to a group of one or more users. Access privileges are determined by the security model parameters (**usm**, **v1**, or **v2**) and security level parameters (**authentication**, **privacy**, or **none**). For each security level, you must associate one MIB view for the group. Associating a MIB view with a group grants the read, write, or notify permission to a set of MIB objects for the group.
- You configure security parameters for each user, including the username, authentication type and authentication password, and privacy type and privacy password. The username given to each user is in a format that is dependent on the security model configured for that user.
- To ensure messaging security, another type of username, called the security name, is included in the messaging data that is sent between the local SNMP server and the destination SNMP server. Each user name is mapped to a security name, but the security name is in a format that is independent of the security model.
- Trap entries in SNMPv3 are created by configuring the notify, notify filter, target address, and target parameters. The **notify** statement specifies the type of notification (trap) and contains a single tag that defines a set of target addresses to receive a trap. The notify filter defines access to a collection of trap object identifiers (OIDs). The target address defines the address of an SNMP management application and other attributes used in sending notifications. Target parameters define the message processing and security parameters used in sending notifications to a particular target.

Copyright © 2018, Juniper Networks, Inc.

Related Documentation

- Assigning a Security Name to a Group on page 268
- Configuring Access Privileges for a Group on page 267
- Configuring SNMP Informs on page 270
- Creating SNMPv3 Users on page 266

Minimum SNMPv3 Configuration on a Device Running Junos OS

To configure the minimum requirements for SNMPv3, include the following statements at the **[edit snmp v3]** and **[edit snmp]** hierarchy levels:

NOTE: You must configure at least one view (notify, read, or write) at the **[edit snmp view-name]** hierarchy level.

```
[edit snmp]
view view-name {
   oid object-identifier (include | exclude);
}
[edit snmp v3]
notify name {
   tag tag-name;
}
notify-filter profile-name {
   oid object-identifier (include | exclude);
}
snmp-community community-index {
   security-name security-name;
}
target-address target-address-name {
   address address;
   target-parameters target-parameters-name;
}
target-parameters target-parameters-name {
   notify-filter profile-name;
   parameters {
      message-processing-model (v1 | v2c | v3);
      security-level (authentication | none | privacy);
      security-model (usm | v1 | v2c);
      security-name security-name;
   }
}
usm {
   local-engine {
      user username {
      }
   }
}
vacm {
   access {
      group group-name {
         (default-context-prefix | context-prefix context-prefix){
```


Copyright © 2018, Juniper Networks, Inc.

```
                security-model (any | usm | v1 | v2c) {
                  security-level (authentication | none | privacy) {
                    notify-view view-name;
                    read-view view-name;
                    write-view view-name;
                  }
                }
              }
            }
          }
          security-to-group {
            security-model (usm | v1 | v2c) {
              security-name security-name {
                group group-name;
              }
            }
          }
        }
```

Related Documentation

- Creating SNMPv3 Users on page 266
- Configuring MIB Views on page 261
- *Defining Access Privileges for an SNMP Group*
- Configuring SNMPv3 Traps on a Device Running Junos OS on page 269
- Configuring SNMP Informs on page 270
- *Example: SNMPv3 Configuration*

Understanding RMON

- RMON Overview on page 217
- Alarm Thresholds and Events on page 218

RMON Overview

The Junos OS supports the *Remote Network Monitoring* (RMON) MIB (RFC 2819), which allows a management device to monitor the values of MIB objects, or variables, against configured thresholds. When the value of a variable crosses a threshold, an alarm and its corresponding event are generated. The event can be logged and can generate an SNMP trap.

An operational support system (OSS) or a fault-monitoring system can be used to automatically monitor events that track many different metrics, including performance, availability, faults, and environmental data. For example, an administrator might want to know when the internal temperature of a chassis has risen above a configured threshold, which might indicate that a chassis fan tray is faulty, the chassis air flow is impeded, or the facility cooling system in the vicinity of the chassis is not operating normally.

The RMON MIB also defines tables that store various statistics for Ethernet interfaces, including the **etherStatsTable** and the **etherHistoryTable**. The **etherStatsTable** contains cumulative real-time statistics for Ethernet interfaces, such as the number of unicast,

multicast, and broadcast packets received on an interface. The **etherHistoryTable** maintains a historical sample of statistics for Ethernet interfaces. The control of the **etherHistoryTable**, including the interfaces to track and the sampling interval, is defined by the RMON **historyControlTable**.

To enable RMON alarms, you perform the following steps:

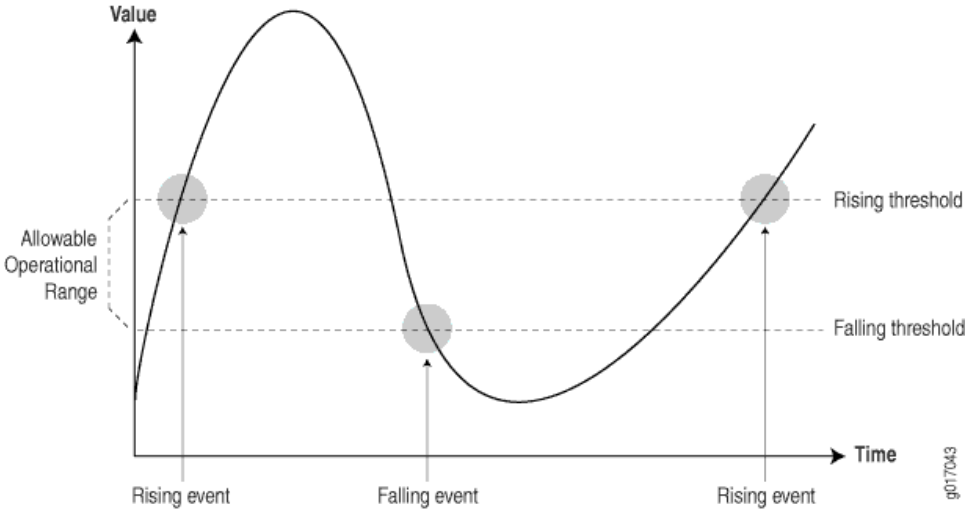
1. Configure SNMP, including trap groups. You configure SNMP at the [**edit snmp**] hierarchy level.
2. Configure rising and falling events in the **eventTable**, including the event types and trap groups. You can also configure events using the CLI at the [**edit snmp rmon event**] hierarchy level.
3. Configure alarms in the **alarmTable**, including the variables to monitor, rising and falling thresholds, the sampling types and intervals, and the corresponding events to generate when alarms occur. You can also configure alarms using the CLI at the [**edit snmp rmon alarm**] hierarchy level.

   Extensions to the **alarmTable** are defined in the Juniper Networks enterprise-specific MIB **jnxRmon** (mib-jnx-rmon.txt).

Alarm Thresholds and Events

By setting a rising and a falling threshold for a monitored variable, you can be alerted whenever the value of the variable falls outside the allowable operational range (see Figure 6 on page 218).

Figure 6: Setting Thresholds



Events are only generated when the alarm threshold is first crossed in any one direction rather than after each sample interval. For example, if a rising threshold alarm, along with its corresponding event, is raised, no more threshold crossing events occur until a corresponding falling alarm occurs. This considerably reduces the quantity of events that are produced by the system, making it easier for operations staff to react when events do occur.

Copyright © 2018, Juniper Networks, Inc.

Before you configure remote monitoring, you should identify what variables need to be monitored and their allowable operational range. This requires some period of baselining to determine the allowable operational ranges. An initial baseline period of at least 3 months is not unusual when you first identify the operational ranges and define thresholds, but baseline monitoring should continue over the life span of each monitored variable.

Related Documentation

- Configuring RMON Alarms and Events on page 262
- Juniper Networks Enterprise-Specific MIBs on page 248
- RMON MIB Event, Alarm, Log, and History Control Tables on page 219

RMON MIB Event, Alarm, Log, and History Control Tables

The Junos OS supports the *Remote Network Monitoring* (RMON) MIB (RFC 2819), which allows a management device to monitor the values of MIB objects, or variables, against configured thresholds. When the value of a variable crosses a threshold, an alarm and its corresponding event are generated. The event can be logged and can generate an SNMP trap.

Table 31 on page 219 provides each field in the RMON eventTable, the description of the field, and the corresponding Junos OS statement that you can use to configure the field. The Junos OS statements reside at the [**edit snmp rmon**] hierarchy level.

Table 31: RMON Event Table

Field	Description	Statement [edit snmp rmon]
eventDescription	Text description of this event.	**description**
eventType	Type of event (for example, log, trap, or log and trap).	**type**
eventCommunity	Trap group to which to send this event, as defined in the Junos OS configuration. (This is not the same as the SNMP community.)	**community**
eventOwner	Entity (for example, manager) that created this event.	—
eventStatus	Status of this row (for example, valid, invalid, or createRequest).	—

Table 32 on page 219 provides each field in the RMON alarmTable, the description of the field, and the corresponding Junos OS statement that you can use to configure the field. The Junos OS statements reside at the [**edit snmp rmon**] hierarchy level.

Table 32: RMON Alarm Table

Field	Description	Statement [edit snmp rmon]
alarmStatus	Status of this row (for example, valid, invalid, or createRequest)	—

Copyright © 2018, Juniper Networks, Inc.

Table 32: RMON Alarm Table *(continued)*

Field	Description	Statement [edit snmp rmon]
alarmInterval	Sampling period (in seconds) of the monitored variable	**interval**
alarmVariable	Object identifier (OID) and instance of the variable to be monitored	—
alarmValue	Actual value of the sampled variable	—
alarmSampleType	Sample type (absolute or delta changes)	**sample-type**
alarmStartupAlarm	Initial alarm (rising, falling, or either)	**startup-alarm**
alarmRisingThreshold	Rising threshold against which to compare the value	**rising-threshold**
alarmFallingThreshold	Falling threshold against which to compare the value	**falling-threshold**
alarmRisingEventIndex	Index (row) of the rising event in the event table	**rising-event-index**
alarmFallingEventIndex	Index (row) of the falling event in the event table	**falling-event-index**

Table 33 on page 220 provides each field in the jnxRmon jnxRmonAlarmTable, which is an extension to the RMON alarmTable. You can troubleshoot the RMON agent, rmopd, that runs on a switch by inspecting the contents of the jnxRmonAlarmTable object.

Table 33: jnxRmon Alarm Table

Field	Description
jnxRmonAlarmGetFailCnt	Number of times the internal **Get** request for the variable failed
jnxRmonAlarmGetFailTime	Value of the sysUpTime object when the last failure occurred
jnxRmonAlarmGetFailReason	Reason why the **Get** request failed
jnxRmonAlarmGetOkTime	Value of the sysUpTime object when the variable moved out of failure state
jnxRmonAlarmState	Status of this alarm entry

Table 34 on page 221 provides each field in the RMON historyControlTable, the description of the field, and the corresponding Junos OS statement that you can use to configure the field. The Junos OS statements reside at the [**edit snmp rmon history**] hierarchy level. The historyControlTable controls the RMON etherHistoryTable.

Copyright © 2018, Juniper Networks, Inc.

Table 34: RMON History Control Table

Field	Description	Statement [edit snmp rmon history]
historyControlDataSource	Identifies the source of the data for which historical data was collected.	**interface**
historyControlBucketsRequested	Requested number of discrete time intervals over which data is to be saved.	**bucket-size**
historyControlBucketsGranted	Number of discrete sampling intervals over which data is to be saved.	—
historyControlInterval	Interval, in seconds, over which the data is sampled for each bucket.	**interval**
historyControlOwner	Entity that configured this entry.	**owner**
historyControlStatus	Status of this entry.	—

Related Documentation

- Configuring RMON Alarms and Events on page 262
- Juniper Networks Enterprise-Specific MIBs on page 248
- Understanding RMON on page 217

Understanding Health Monitoring

Health monitoring is an SNMP feature that extends the RMON alarm infrastructure to provide monitoring for a predefined set of objects (such as file system usage, CPU usage, and memory usage), and for Junos OS processes.

You enable the health monitor feature using the **health-monitor** statement at the **[edit snmp]** hierarchy level. You can also configure health monitor parameters such as a falling threshold, rising threshold, and interval. If the value of a monitored object exceeds the rising or falling threshold, an alarm is triggered and an event may be logged.

The falling threshold is the lower threshold for the monitored object instance. The rising threshold is the upper threshold for the monitored object instance. Each threshold is expressed as a percentage of the maximum possible value. The interval represents the period of time, in seconds, over which the object instance is sampled and compared with the rising and falling thresholds.

Events are only generated when a threshold is first crossed in any one direction, rather than after each sample interval. For example, if a rising threshold alarm, along with its corresponding event, is raised, no more threshold crossing events occur until a corresponding falling alarm occurs.

System log entries for health monitor events have a corresponding HEALTHMONITOR tag and not a generic SNMPD_RMON_EVENTLOG tag. However, the health monitor sends generic RMON risingThreshold and fallingThreshold traps. You can use the **show snmp**

health-monitor operational command to view information about health monitor alarms and logs.

When you configure the health monitor, monitoring information for certain object instances is available, as shown in Table 35 on page 222.

Table 35: Monitored Object Instances

Object	Description
jnxHrStoragePercentUsed.1	Monitors the **/dev/ad0s1a:** file system on the switch. This is the root file system mounted on /.
jnxHrStoragePercentUsed.2	Monitors the **/dev/ad0s1e:** file system on the switch. This is the configuration file system mounted on **/config**.
jnxOperatingCPU (RE0)	Monitors CPU usage by the Routing Engine (RE0).
jnxOperatingBuffer (RE0)	Monitors the amount of memory available on the Routing Engine (RE0).
sysApplElmtRunCPU	Monitors the CPU usage for each Junos OS process (also called daemon). Multiple instances of the same process are monitored and indexed separately.
sysApplElmtRunMemory	Monitors the memory usage for each Junos OS process. Multiple instances of the same process are monitored and indexed separately.

Related Documentation

- Configuring Health Monitoring on page 265
- **falling-threshold (Health Monitor) on page 309**
- **interval (Health Monitor) on page 319**
- **rising-threshold (Health Monitor) on page 342**
- **show snmp health-monitor on page 397**

Copyright © 2018, Juniper Networks, Inc.

SNMP MIBs Support

The QFX Series standalone switches, QFX Series Virtual Chassis, and QFabric systems support standard MIBs and Juniper Networks enterprise-specific MIBs.

NOTE: For information about enterprise-specific SNMP MIB objects, see the SNMP MIB Explorer. You can use SNMP MIB Explorer to view information about various MIBs, MIB objects, and SNMP notifications supported on Juniper Networks devices

For more information, see:

- MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis on page 223
- MIBs Supported on QFabric Systems on page 230

MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis

The QFX Series standalone switches and QFX Series Virtual Chassis support both standard MIBs and Juniper Networks enterprise-specific MIBs. For more information, see:

- Table 36 on page 223 for standard MIBs.
- Table 37 on page 229 for Juniper Networks enterprise-specific MIBs.

Table 36: Standard MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis

RFC	Additional Information
IEEE 802.1ab section 12.1, *Link Layer Discovery Protocol (LLDP) MIB*	Supported tables and objects: • lldpRemManAddrOID • lldpLocManAddrOID • lldpReinitDelay • lldpNotificationInterval • lldpStatsRxPortFramesDiscardedTotal • lldpStatsRxPortFramesError • lldpStatsRxPortTLVsDiscardedTotal • lldpStatsRxPortTLVsUnrecognizedTotal • lldpStatsRxPortAgeoutsTotal

Table 36: Standard MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

RFC	Additional Information
IEEE 802.3ad, *Aggregation of Multiple Link Segments*	The following tables and objects are supported: • dot3adAggPortTable, dot3adAggPortListTable, dot3adAggTable, and dot3adAggPortStatsTable • dot3adAggPortDebugTable (only dot3adAggPortDebugRxState, dot3adAggPortDebugMuxState, dot3adAggPortDebugActorSyncTransitionCount, dot3adAggPortDebugPartnerSyncTransitionCount, dot3adAggPortDebugActorChangeCount, and dot3adAggPortDebugPartnerChangeCount) • dot3adTablesLastChanged
RFC 1155, *Structure and Identification of Management Information for TCP/IP-based Internets*	—
RFC 1157, *A Simple Network Management Protocol (SNMP)*	—
RFC 1212, *Concise MIB Definitions*	—

RFC 1213, *Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II*	The following areas are supported:
	• MIB II and its SNMP version 2 derivatives, including:
	  ◦ Statistics counters
	  ◦ IP, except for ipRouteTable, which has been replaced by ipCidrRouteTable (RFC 2096, *IP Forwarding Table MIB*)
	  ◦ ipAddrTable
	  ◦ SNMP management
	  ◦ Interface management
	• SNMPv1 **Get**, **GetNext** requests, and SNMPv2 **GetBulk** request
	• Junos OS-specific secured access list
	• Master configuration keywords
	• Reconfigurations upon SIGHUP

RFC 1215, *A Convention for Defining Traps for use with the SNMP*	Support is limited to MIB II SNMP version 1 traps and version 2 notifications.
RFC 1286, *Definitions of Managed Objects for Bridges*	—
RFC 1657, *Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2*	—

Copyright © 2018, Juniper Networks, Inc.

Table 36: Standard MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

RFC	Additional Information
RFC 1850, *OSPF Version 2 Management Information Base*	The following table, objects, and traps are not supported: • Host Table • ospfOriginateNewLsas and ospfRxNewLsas objects • ospfOriginateLSA, ospfLsdbOverflow, and ospfLsdbApproachingOverflow traps
RFC 1901, *Introduction to Community-based SNMPv2*	—
RFC 1905, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*	—
RFC 1907, *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)*	—
RFC 2011, *SNMPv2 Management Information Base for the Internet Protocol Using SMIv2*	—
RFC 2012, *SNMPv2 Management Information Base for the Transmission Control Protocol Using SMIv2*	—
RFC 2013, *SNMPv2 Management Information Base for the User Datagram Protocol Using SMIv2*	—
RFC 2233, *The Interfaces Group MIB Using SMIv2*	NOTE: RFC 2233 has been replaced by RFC 2863. However, Junos OS supports both RFC 2233 and RFC 2863.
RFC 2287, *Definitions of System-Level Managed Objects for Applications*	The following objects are supported: • sysApplInstallPkgTable • sysApplInstallElmtTable • sysApplElmtRunTable • sysApplMapTable
RFC 2570, *Introduction to Version 3 of the Internet-standard Network Management Framework*	—
RFC 2571, *An Architecture for Describing SNMP Management Frameworks* (read-only access)	NOTE: RFC 2571 has been replaced by RFC 3411. However, Junos OS supports both RFC 2571 and RFC 3411.
RFC 2572, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* (read-only access)	NOTE: RFC 2572 has been replaced by RFC 3412. However, Junos OS supports both RFC 2572 and RFC 3412.

Copyright © 2018, Juniper Networks, Inc.

Table 36: Standard MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

RFC	Additional Information
RFC 2576, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*	NOTE: RFC 2576 has been replaced by RFC 3584. However, Junos OS supports both RFC 2576 and RFC 3584.
RFC 2578, *Structure of Management Information Version 2 (SMIv2)*	—
RFC 2579, *Textual Conventions for SMIv2*	—
RFC 2580, *Conformance Statements for SMIv2*	—
RFC 2665, *Definitions of Managed Objects for the Ethernet-like Interface Types*	—
RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol*	Support does not include row creation, the Set operation, and the vrrpStatsPacketLengthErrors object.
RFC 2790, *Host Resources MIB*	Support is limited to the following objects: • Only hrStorageTable. The file systems **/**, **/config**, **/var**, and **/tmp** always return the same index number. When SNMP restarts, the index numbers for the remaining file systems might change. • Only the objects of the hrSystem and hrSWInstalled groups.
RFC 2819, *Remote Network Monitoring Management Information Base*	The following objects are supported: • etherStatsTable (for Ethernet interfaces only), alarmTable, eventTable, and logTable. • historyControlTable and etherHistoryTable (except the etherHistoryUtilization object).
RFC 2863, *The Interfaces Group MIB*	NOTE: RFC 2233 has been replaced by RFC 2863. However, Junos OS supports both RFC 2233 and RFC 2863.
RFC 2932, *IPv4 Multicast Routing MIB*	—
RFC 2933, *Internet Group Management Protocol (IGMP) MIB*	—
RFC 2934, *Protocol Independent Multicast MIB for IPv4*	In Junos OS, RFC 2934 is implemented based on a draft version, *pimmib.mib*, of the now standard RFC.
RFC 3410, *Introduction and Applicability Statements for Internet Standard Management Framework*	—

Copyright © 2018, Juniper Networks, Inc.

Table 36: Standard MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

RFC	Additional Information
RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*	NOTE: RFC 3411 replaces RFC 2571. However, Junos OS supports both RFC 3411 and RFC 2571.
RFC 3412, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*	NOTE: RFC 3412 replaces RFC 2572. However, Junos OS supports both RFC 3412 and RFC 2572.
RFC 3413, *Simple Network Management Protocol (SNMP) Applications*	All MIBs are supported except for the Proxy MIB.
RFC 3414, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*	—
RFC 3415, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*	—
RFC 3416, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*	NOTE: RFC 3416 replaces RFC 1905, which was supported in earlier versions of Junos OS.
RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP)*	—
RFC 3418, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*	NOTE: RFC 3418 replaces RFC 1907, which was supported in earlier versions of Junos OS.
RFC 3584, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*	—
RFC 3826, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*	—

Copyright © 2018, Juniper Networks, Inc.

Table 36: Standard MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

RFC	Additional Information
RFC 4188, *Definitions of Managed Objects for Bridges*	The QFX3500 and QFX3600 switches support 802.1D STP (1998) and the following subtrees and objects only: • dot1dTp subtree—dot1dTpFdbAddress, dot1dTpFdbPort, and dot1dTpFdbStatus objects from the dot1dTpFdbTable table. • dot1dBase subtree—dot1dBasePort and dot1dBasePortIfIndex objects from the dot1dBasePortTable table. NOTE: On QFX3500 and QFX3600 switches, the dot1dTpFdbTable table is populated only with MAC addresses learned on the default VLAN. To see the MAC addresses of all VLANs, specify the dot1qTpFdbTable table (RFC 4363b, *Q-Bridge VLAN MIB*) when you issue the **show snmp mib walk** command. Not supported on OCX Series devices.
RFC 4293, *Management Information Base for the Internet Protocol (IP)*	Supports the ipAddrTable table only.
RFC 4318, *Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol*	Supports 802.1w and 802.1t extensions for RSTP. Not supported on OCX Series devices.
RFC 4363b, *Q-Bridge VLAN MIB*	NOTE: On QFX3500 and QFX3600 switches, the dot1dTpFdbTable table (RFC 4188, *Definitions of Managed Objects for Bridges*) is populated only with MAC addresses learned on the default VLAN. To see the MAC addresses of all VLANs, specify the dot1qTpFdbTable table (in this MIB) when you issue the **show snmp mib walk** command. Not supported on OCX Series devices.
RFC 4444, *IS-IS MIB*	—
Internet Assigned Numbers Authority, *IANAiftype Textual Convention MIB* (referenced by RFC 2233)	See http://www.iana.org/assignments/ianaiftype-mib .
Internet draft draft-reeder-snmpv3-usm-3desede-00.txt, *Extension to the User-Based Security Model (USM) to Support Triple-DES EDE in 'Outside' CBC Mode*	—
Internet draft draft-ietf-idmr-igmp-mib-13.txt, *Internet Group Management Protocol (IGMP) MIB*	—
ESO Consortium MIB	NOTE: The ESO Consortium MIB has been replaced by RFC 3826. See http://www.snmp.com/eso/.

Copyright © 2018, Juniper Networks, Inc.

Table 37: Juniper Networks Enterprise-Specific MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis

MIB	Description
Alarm MIB (mib-jnx-chassis-alarm)	Provides support for alarms from the switch.
Analyzer MIB (mib-jnx-analyzer)	Contains analyzer and remote analyzer data related to port mirroring. Not supported on OCX Series devices.
Chassis MIB (mib-jnx-chassis)	Provides support for environmental monitoring (power supply state, board voltages, fans, temperatures, and airflow) and inventory support for the chassis, Flexible PIC Concentrators (FPCs), and PICs. NOTE: The jnxLEDTable table has been deprecated.
Chassis Definitions for Router Model MIB (mib-jnx-chas-defines)	Contains the object identifiers (OIDs) that are used by the Chassis MIB to identify routing and switching platforms and chassis components. The Chassis MIB provides information that changes often, whereas the Chassis Definitions for Router Model MIB provides information that changes less often.
Class-of-Service MIB (mib-jnx-cos)	Provides support for monitoring interface output queue statistics per interface and per forwarding class.
Configuration Management MIB (mib-jnx-cfgmgmt)	Provides notification for configuration changes and rescue configuration changes in the form of SNMP traps. Each trap contains the time at which the configuration change was committed, the name of the user who made the change, and the method by which the change was made. A history of the last 32 configuration changes is kept in jnxCmChgEventTable.
Ethernet MAC MIB (mib-jnx-mac)	Monitors media access control (MAC) statistics on Gigabit Ethernet intelligent queuing (IQ) interfaces. It collects MAC statistics; for example, inoctets, inframes, outoctets, and outframes on each source MAC address and virtual LAN (VLAN) ID for each Ethernet port. Not supported on OCX Series devices.
Event MIB (mib-jnx-event)	Defines a generic trap that can be generated using an operations script or event policy. This MIB provides the ability to specify a system log string and raise a trap if that system log string is found. In Junos OS release 13.2X51-D10 or later, if you configured an event policy to raise a trap when a new SNMP trap target is added, the SNMPD_TRAP_TARGET_ADD_NOTICE trap is generated with information about the new target.
Firewall MIB (mib-jnx-firewall)	Provides support for monitoring firewall filter counters.
Host Resources MIB (mib-jnx-hostresources)	Extends the hrStorageTable object, providing a measure of the usage of each file system on the switch as a percentage. Previously, the objects in the hrStorageTable measured the usage in allocation units—hrStorageUsed and hrStorageAllocationUnits—only. Using the percentage measurement, you can more easily monitor and apply thresholds on usage.
Interface MIB (Extensions) (mib-jnx-if-extensions)	Extends the standard ifTable (RFC 2863) with additional statistics and Juniper Networks enterprise-specific chassis information in the ifJnxTable and ifChassisTable tables.

Table 37: Juniper Networks Enterprise-Specific MIBs Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

MIB	Description
L2ALD MIB (mib-jnx-l2ald)	Provides information about Layer 2 Address Learning and related traps, such as the routing instance MAC limit trap and interface MAC limit trap. This MIB also provides VLAN information in the jnxL2aldVlanTable table for Enhanced Layer 2 Software (ELS) EX Series and QFX Series switches. NOTE: Non-ELS EX Series switches use the VLAN MIB (jnxExVlanTable) for VLAN information instead of this MIB.
MPLS MIB (mib-jnx-mpls)	Provides MPLS information and defines MPLS notifications. NOTE: This MIB is not supported on the QFX5100 switch.
MPLS LDP MIB (mib-jnx-mpls-ldp)	Contains object definitions as described in RFC 3815, *Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)*. NOTE: This MIB is not supported on the QFX5100 switch.
Ping MIB (mib-jnx-ping)	Extends the standard Ping MIB control table (RFC 2925). Items in this MIB are created when entries are created in pingCtlTable of the Ping MIB. Each item is indexed exactly as it is in the Ping MIB.
RMON Events and Alarms MIB (mib-jnx-rmon)	Supports Junos OS extensions to the standard Remote Monitoring (RMON) Events and Alarms MIB (RFC 2819). The extension augments the alarmTable object with additional information about each alarm. Two additional traps are also defined to indicate when problems are encountered with an alarm.
Structure of Management Information MIB (mib-jnx-smi)	Explains how the Juniper Networks enterprise-specific MIBs are structured.
System Log MIB (mib-jnx-syslog)	Enables notification of an SNMP trap-based application when an important system log message occurs.
Utility MIB (mib-jnx-util)	Provides you with SNMP MIB container objects of the following types: 32-bit counters, 64-bit counters, signed integers, unsigned integers, and octet strings. You can use these objects to store data that can be retrieved using other SNMP operations.
VLAN MIB (mib-jnx-vlan)	Contains information about prestandard IEEE 802.10 VLANs and their association with LAN emulation clients. NOTE: For ELS EX Series switches and QFX Series switches, VLAN information is available in the L2ALD MIB in the jnxL2aldVlanTable table instead of in the VLAN MIB For non-ELS EX Series switches, VLAN information is provided in the VLAN MIB in the jnxExVlanTable table. Not supported on OCX Series devices.

MIBs Supported on QFabric Systems

The QFabric systems support both standard MIBs and Juniper Networks enterprise-specific MIBs. For more information, see:

Copyright © 2018, Juniper Networks, Inc.

- Table 38 on page 231 for standard MIBs.
- Table 39 on page 234 for Juniper Networks enterprise-specific MIBs.

Table 38: Standard MIBs Supported on QFabric Systems

RFC	Additional Information
RFC 1155, *Structure and Identification of Management Information for TCP/IP-based Internets*	—
RFC 1157, *A Simple Network Management Protocol (SNMP)*	—
RFC 1212, *Concise MIB Definitions*	—

RFC 1213, *Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II*	The following areas are supported:
	• MIB II and its SNMP version 2 derivatives, including:
	  • Statistics counters
	  • IP, except for ipRouteTable, which has been replaced by ipCidrRouteTable (RFC 2096, *IP Forwarding Table MIB*)
	  • ipAddrTable
	  • SNMP management
	  • Interface management
	• SNMPv1 **Get**, **GetNext** requests, and version 2 **GetBulk** request
	• Junos OS-specific secured access list
	• Master configuration keywords
	• Reconfigurations upon SIGHUP

RFC 1215, *A Convention for Defining Traps for use with the SNMP*	Support is limited to MIB II SNMP version 1 traps and version 2 notifications.
RFC 1286, *Definitions of Managed Objects for Bridges*	—
RFC 1901, *Introduction to Community-based SNMPv2*	—
RFC 1905, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*	—
RFC 1907, *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)*	—
RFC 2011, *SNMPv2 Management Information Base for the Internet Protocol Using SMIv2*	NOTE: On the QFabric system, for the SNMP mibwalk request to work, you must configure the IP address of at least one interface besides the management Ethernet interfaces (me0 and me1) in the Director group.

Copyright © 2018, Juniper Networks, Inc.

Table 38: Standard MIBs Supported on QFabric Systems *(continued)*

RFC	Additional Information
RFC 2012, *SNMPv2 Management Information Base for the Transmission Control Protocol Using SMIv2*	—
RFC 2013, *SNMPv2 Management Information Base for the User Datagram Protocol Using SMIv2*	—
RFC 2233, *The Interfaces Group MIB Using SMIv2*	NOTE: RFC 2233 has been replaced by RFC 2863. However, Junos OS supports both RFC 2233 and RFC 2863. NOTE: The QFabric system supports the following objects only: ifNumber, ifTable, and ifxTable.
RFC 2571, *An Architecture for Describing SNMP Management Frameworks* (read-only access)	NOTE: RFC 2571 has been replaced by RFC 3411. However, Junos OS supports both RFC 2571 and RFC 3411.
RFC 2572, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* (read-only access)	NOTE: RFC 2572 has been replaced by RFC 3412. However, Junos OS supports both RFC 2572 and RFC 3412.
RFC 2576, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*	NOTE: RFC 2576 has been replaced by RFC 3584. However, Junos OS supports both RFC 2576 and RFC 3584.
RFC 2578, *Structure of Management Information Version 2 (SMIv2)*	—
RFC 2579, *Textual Conventions for SMIv2*	—
RFC 2580, *Conformance Statements for SMIv2*	—
RFC 2665, *Definitions of Managed Objects for the Ethernet-like Interface Types*	The QFabric system supports the following tables only: • dot3StatsTable—There is one row with statistics for each Ethernet-like interface in the QFabric system. The dot3StatsIndex is an interface index that is unique across the system. • dot3ControlTable—There is one row in this table for each Ethernet-like interface in the QFabric system that implements the MAC control sublayer. OIDs supported are dot3ControlFunctionsSupported and dot3ControlInUnknownOpcode. • dot3PauseTable—There is one row in this table for each Ethernet-like interface in the QFabric system that supports the MAC control PAUSE function. OIDs supported are dot3PauseAdminMode, dot3PauseOperMode, dot3InPauseFrames, and dot3OutPauseFrames. NOTE: Scalar variables are not supported on the QFabric system.

Copyright © 2018, Juniper Networks, Inc.

Table 38: Standard MIBs Supported on QFabric Systems *(continued)*

RFC	Additional Information
RFC 2863, *The Interfaces Group MIB*	NOTE: RFC 2233 has been replaced by RFC 2863. However, Junos OS supports both RFC 2233 and RFC 2863. NOTE: The QFabric system supports the following objects only: ifNumber, ifTable, and ifxTable.
RFC 2933, *Internet Group Management Protocol (IGMP) MIB*	—
RFC 3410, *Introduction and Applicability Statements for Internet Standard Management Framework*	—
RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*	NOTE: RFC 3411 replaces RFC 2571. However, Junos OS supports both RFC 3411 and RFC 2571.
RFC 3412, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*	NOTE: RFC 3412 replaces RFC 2572. However, Junos OS supports both RFC 3412 and RFC 2572.
RFC 3416, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*	NOTE: RFC 3416 replaces RFC 1905, which was supported in earlier versions of Junos OS.
RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP)*	—
RFC 3418, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*	NOTE: RFC 3418 replaces RFC 1907, which was supported in earlier versions of Junos OS.
RFC 3584, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*	—
RFC 4188, *Definitions of Managed Objects for Bridges*	The QFabric system support is limited to the following objects: • Under the dot1dBase OID, the dot1dBasePortTable table supports only the first two columns in the table: dot1dBasePort and dot1dBasePortIfIndex. • The system does not implement the optional traps supporting dot1dNotifications (dot1dBridge 0). • Under the dot1dStp OID, supports only the dot1dStpPortTable table. Does not support the scalar variables under dot1dStp. • The system does not support scalar variables under dot1dTp, but under that, the dot1dTpFdbTable table is supported (dot1dBridge 4). • For OIDS with tables support only, scalar values that are returned by the SNMP agent may not be meaningful and are therefore not recommended for use. Not supported on OCX Series devices.

Table 38: Standard MIBs Supported on QFabric Systems *(continued)*

RFC	Additional Information
RFC 4293, *Management Information Base for the Internet Protocol (IP)*	Supports the ipAddrTable table only. On the QFabric system, supported objects in the ipAddrTable table include: ipAdEntAddr, ipAdEntIfIndex, ipAdEntNetMask, ipAdEntBcastAddr, and ipAdEntReasmMaxSize. NOTE: On the QFabric system, for the SNMP mibwalk request to work, you must configure the IP address of at least one interface besides the management Ethernet interfaces (me0 and me1) in the Director group.
RFC 4363b, *Q-Bridge VLAN MIB*	The QFabric system supports the following tables only: • dot1qTpFdbTable • dot1qVlanStaticTable • dot1qPortVlanTable • dot1qFdbTable Not supported on OCX Series devices.

NOTE: **QFabric-specific MIBs are not supported on OCX Series devices.**

Table 39: Juniper Networks Enterprise-Specific MIBs Supported on QFabric Systems

MIB	Description
Analyzer MIB (mib-jnx-analyzer)	Contains analyzer and remote analyzer data related to port mirroring. The QFabric system supports: • Analyzer table—jnxAnalyzerName, jnxMirroringRatio, jnxLossPriority. • Analyzer input table—jnxAnalyzerInputValue, jnxAnalyzerInputOption, jnxAnalyzerInputType. • Analyzer output table—jnx AnalyzerOutputValue, jnxAnalyzerOutputType.
Chassis MIB (mib-jnx-chassis)	NOTE: The Chassis MIB has been deprecated for the QFabric system. We recommend that you use the Fabric Chassis MIB (mib-jnx-fabric-chassis) for information about the QFabric system.
Class-of-Service MIB (mib-jnx-cos)	Provides support for monitoring interface output queue statistics per interface and per forwarding class. The QFabric system supports the following tables and objects: • Jnxcosifstatflagtable—jnxCosIfstatFlags and jnxCosIfIndex. • Jnxcosqstattable—jnxCosQstatTxedPkts, jnxCosQstatTxedPktRate, jnxCosQstatTxedBytes, and jnxCosQstatTxedByteRate. • Jnxcosfcidtable—jnxCosFcIdToFcName. • Jnxcosfctable—jnxCosFcQueueNr. The QFabric system does not support any traps for this MIB.

Copyright © 2018, Juniper Networks, Inc.

Table 39: Juniper Networks Enterprise-Specific MIBs Supported on QFabric Systems *(continued)*

MIB	Description
Configuration Management MIB (mib-jnx-cfgmgmt)	Provides notification for configuration changes and rescue configuration changes in the form of SNMP traps. Each trap contains the time at which the configuration change was committed, the name of the user who made the change, and the method by which the change was made. A history of the last 32 configuration changes is kept in jnxCmChgEventTable. NOTE: On the QFabric system, these conditions apply: • All scalar variables under the jnxCmCfgChg table are supported. • Supported scalar OIDs are jnxCmCfgChgLatestIndex, jnxCmCfgChgLatestTime, jnxCmCfgChgLatestDate, jnxCmCfgChgLatestSource, jnxCmCfgChgLatestUser, and jnxCmCfgChgMaxEventEntries. • Scalar variables under the jnxCmRescueChg table are not supported.
Fabric Chassis MIB (mib-jnx-fabric-chassis)	Provides hardware information about the QFabric system and its component devices. This MIB is based on the Juniper Networks enterprise-specific Chassis MIB but adds another level of indexing that provides information for QFabric system component devices.
Interface MIB (Extensions) (mib-jnx-if-extensions)	Extends the standard ifTable (RFC 2863) with additional statistics and Juniper Networks enterprise-specific chassis information in the ifJnxTable and ifChassisTable tables. NOTE: On the QFabric system, scalar variables are not supported.
Power Supply Unit MIB (mib-jnx-power-supply-unit)	Provides support for environmental monitoring of the power supply unit for the Interconnect device of the QFabric system. NOTE: On the QFabric system, scalar variables for the jnxPsuObjects 1 object ID in the jnxPsuScalars table are not supported.
QFabric MIB (jnx-qf-smi)	Explains how the Juniper Networks enterprise-specific QFabric MIBs are structured. Defines the MIB objects that are reported by the QFabric system and the contents of the traps that can be issued by the QFabric system.
Utility MIB (mib-jnx-util)	Provides you with SNMP MIB container objects of the following types: 32-bit counters, 64-bit counters, signed integers, unsigned integers, and octet strings. You can use these objects to store data that can be retrieved using other SNMP operations.

Related Documentation

- SNMP MIB Explorer
- Understanding the Implementation of SNMP on page 212
- *Understanding the Implementation of SNMP on the QFabric System*
- SNMP Traps Support on page 236

SNMP Traps Support

The QFX Series standalone switches, QFX Series Virtual Chassis, and QFabric systems support standard SNMP traps and Juniper Networks enterprise-specific traps.

For more information, see:

- SNMP Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis on page 236
- SNMP Traps Supported on QFabric Systems on page 244

SNMP Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis

QFX Series standalone switches and QFX Series Virtual Chassis support SNMPv1 and v2 traps. For more information, see:

- SNMPv1 Traps on page 236
- SNMPv2 Traps on page 240

SNMPv1 Traps

QFX Series standalone switches and QFX Series Virtual Chassis support both standard SNMPv1 traps and Juniper Networks enterprise-specific SNMPv1 traps. See:

- Table 40 on page 236 for standard SNMPv1 traps.
- Table 41 on page 239 for enterprise-specific SNMPv1 traps.

The traps are organized first by trap category and then by trap name. The system logging severity levels are listed for those traps that have them. Traps that do not have corresponding system logging severity levels are marked with an en dash (–).

Table 40: Standard SNMP Version 1 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	Syslog Tag
Link Notifications						
RFC 1215, *Conventions for Defining Traps for Use with the SNMP*	linkDown	1.3.6.1.4.1.2636	2	0	Warning	SNMP_ TRAP_ LINK_DOWN
	linkUp	1.3.6.1.4.1.2636	3	0	Info	SNMP_TRAP_ LINK_UP
Remote Operations Notifications						
RFC 2925, *Definitions of Managed Objects*	pingProbeFailed	1.3.6.1.2.1.80.0	6	1	Info	SNMP_TRAP _PING_ PROBE_ FAILED

Copyright © 2018, Juniper Networks, Inc.

Table 40: Standard SNMP Version 1 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	Syslog Tag
for Remote Ping, Traceroute, and Lookup Operations	pingTestFailed	1.3.6.1.2.1.80.0	6	2	Info	SNMP_TRAP_ PING_TEST _FAILED
	pingTestCompleted	1.3.6.1.2.1.80.0	6	3	Info	SNMP_TRAP_ PING_TEST_ COMPLETED
	traceRoutePathChange	1.3.6.1.2.1.81.0	6	1	Info	SNMP_TRAP_ TRACE_ROUTE_ PATH_CHANGE
	traceRouteTestFailed	1.3.6.1.2.1.81.0	6	2	Info	SNMP_TRAP_ TRACE_ROUTE_ TEST_FAILED
	traceRouteTestCompleted	1.3.6.1.2.1.81.0	6	3	Info	SNMP_TRAP_ TRACE_ROUTE_ TEST_COMPLETED
RMON Alarms						
RFC 2819a, *RMON MIB*	fallingAlarm	1.3.6.1.2.1.16	6	2	–	–
	risingAlarm	1.3.6.1.2.1.16	6	1	–	–
Routing Notifications						
BGP 4 MIB	bgpEstablished	1.3.6.1.2.1.15.7	6	1	–	–
	bgpBackwardTransition	1.3.6.1.2.1.15.7	6	2	–	–

Table 40: Standard SNMP Version 1 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	Syslog Tag
OSPF TRAP MIB	ospfVirtIfStateChange	1.3.6.1.2.1.14.16.2	6	1	–	–
	ospfNbrStateChange	1.3.6.1.2.1.14.16.2	6	2	–	–
	ospfVirtNbrStateChange	1.3.6.1.2.1.14.16.2	6	3	–	–
	ospfIfConfigError	1.3.6.1.2.1.14.16.2	6	4	–	–
	ospfVirtIfConfigError	1.3.6.1.2.1.14.16.2	6	5	–	–
	ospfIfAuthFailure	1.3.6.1.2.1.14.16.2	6	6	–	–
	ospfVirtIfAuthFailure	1.3.6.1.2.1.14.16.2	6	7	–	–
	ospfIfRxBadPacket	1.3.6.1.2.1.14.16.2	6	8	–	–
	ospfVirtIfRxBadPacket	1.3.6.1.2.1.14.16.2	6	9	–	–
	ospfTxRetransmit	1.3.6.1.2.1.14.16.2	6	10	–	–
	ospfVirtIfTxRetransmit	1.3.6.1.2.1.14.16.2	6	11	–	–
	ospfMaxAgeLsa	1.3.6.1.2.1.14.16.2	6	13	–	–
	ospfIfStateChange	1.3.6.1.2.1.14.16.2	6	16	–	–
Startup Notifications						
RFC 1215, *Conventions for Defining Traps for Use with the SNMP*	authenticationFailure	1.3.6.1.4.1.2636	4	0	Notice	SNMPD_ TRAP_ GEN_FAILURE
	coldStart	1.3.6.1.4.1.2636	0	0	Critical	SNMPD_TRAP_ COLD_START
	warmStart	1.3.6.1.4.1.2636	1	0	Error	SNMPD_TRAP_ WARM_START
VRRP Notifications						
RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol*	vrrpTrapNewMaster	1.3.6.1.2.1.68	6	1	Warning	VRRPD_NEW MASTER_TRAP
	vrrpTrapAuthFailure	1.3.6.1.2.1.68	6	2	Warning	VRRPD_AUTH_ FAILURE_TRAP

Copyright © 2018, Juniper Networks, Inc.

Table 41: Enterprise-Specific SNMPv1 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag
Chassis Notifications (Alarm Conditions)						
Chassis MIB (jnx-chassis. mib)	jnxPowerSupplyFailure	1.3.6.1.4.1.2636.4.1	6	1	Warning	CHASSISD_ SNMP_ TRAP
	jnxFanFailure	1.3.6.1.4.1.26361	6	2	Critical	CHASSISD_ SNMP_ TRAP
	jnxOverTemperature	11.4.1.2636.4.1	6	3	Alert	CHASSISD_ SNMP_ TRAP
	jnxFruRemoval	1.3.6.1.4.1.2636.4.1	6	5	Notice	CHASSISD_ SNMP_ TRAP
	jnxFruInsertion	1.3.6.1.4.1.2636.4.1	6	6	Notice	CHASSISD_ SNMP_ TRAP
	jnxFruPowerOff	1.3.6.1.4.1.2636.4.1	6	7	Notice	CHASSISD_ SNMP_ TRAP
	jnxFruPowerOn	1.3.6.1.4.1.2636.4.1	6	8	Notice	CHASSISD_ SNMP_ TRAP
	jnxFruFailed	1.3.6.1.4.1.2636.4.1	6	9	Warning	CHASSISD_ SNMP_ TRAP
	jnxFruOffline	1.3.6.1.4.1.2636.4.1	6	10	Notice	CHASSISD_ SNMP_ TRAP
	jnxFruOnline	1.3.6.1.4.1.2636.4.1	6	11	Notice	CHASSISD_ SNMP_ TRAP
	jnxFruCheck	1.3.6.1.4.1.2636.4.1	6	12	Warning	CHASSISD_ SNMP_ TRAP
	jnxPowerSupplyOk	1.3.6.1.4.1.2636.4.2	6	1	Critical	CHASSISD_ SNMP_ TRAP
	jnxFanOK	1.3.6.1.4.1.2636.4.2	6	2	Critical	CHASSISD_ SNMP_ TRAP
	jnxTemperatureOK	1.3.6.1.4.1.2636.4.2	6	3	Alert	CHASSISD_ SNMP_ TRAP
Configuration Notifications						

Copyright © 2018, Juniper Networks, Inc.

Table 41: Enterprise-Specific SNMPv1 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

Defined in	Trap Name	Enterprise ID	Generic Trap Number	Specific Trap Number	System Logging Severity Level	System Log Tag
Configuration Management MIB (jnx- configmgmt. mib)	jnxCmCfgChange	1.3.6.1.4.1.2636.4.5	6	1	–	–
	jnxCmRescueChange	1.3.6.1.4.1.2636.4.5	6	2	–	–
Remote Operations						
Ping MIB (jnx-ping.mib)	jnxPingRttThresholdExceeded	1.3.6.1.4.1.2636.4.9	6	1	–	–
	jnxPingRttStdDevThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	2	–	–
	jnxPingRttJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	3	–	–
	jnxPingEgressThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	4	–	–
	jnxPingEgressStdDev ThresholdExceeded	1.3.6.1.4.1.2636.4.9	6	5	–	–
	jnxPingEgressJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	6	–	–
	jnxPingIngressThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	7	–	–
	jnxPingIngressStddevThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	8	–	–
	jnxPingIngressJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9	6	9	–	–
RMON Alarms						
RMON MIB (jnx-rmon. mib)	jnxRmonAlarmGetFailure	1.3.6.1.4.1.2636.4.3	6	1	–	–
	jnxRmonGetOk	1.3.6.1.4.1.2636.4.3	6	2	–	–

SNMPv2 Traps

- Table 42 on page 241 lists the standard SNMP traps
- Table 43 on page 243 lists the Juniper Networks enterprise-specific traps

Copyright © 2018, Juniper Networks, Inc.

Table 42: Standard SNMPv2 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis

Defined in	Trap Name	SNMP Trap OID	System Logging Severity Level	Syslog Tag
Link Notifications				
RFC 2863, *The Interfaces Group MIB*	linkDown	1.3.6.1.6.3.1.1.5.3	Warning	SNMP_TRAP_ LINK_DOWN
	linkUp	1.3.6.1.6.3.1.1.5.4	Info	SNMP_TRAP_ LINK_UP
Remote Operations Notifications				
RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*	pingProbeFailed	1.3.6.1.2.1.80.0.1	Info	SNMP_TRAP_ PING_PROBE_ FAILED
	pingTestFailed	1.3.6.1.2.1.80.0.2	Info	SNMP_TRAP_PING_ TEST_FAILED
	pingTestCompleted	1.3.6.1.2.1.80.0.3	Info	SNMP_TRAP_PING_ TEST_COMPLETED
	traceRoutePathChange	1.3.6.1.2.1.81.0.1	Info	SNMP_TRAP_TRACE_ ROUTE_PATH_ CHANGE
	traceRouteTestFailed	1.3.6.1.2.1.81.0.2	Info	SNMP_TRAP_TRACE_ ROUTE_TEST_FAILED
	traceRouteTestCompleted	1.3.6.1.2.1.81.0.3	Info	SNMP_TRAP_TRACE_ ROUTE_TEST_ COMPLETED
RMON Alarms				
RFC 2819a, *RMON MIB*	fallingAlarm	1.3.6.1.2.1.16.0.1	–	–
	risingAlarm	1.3.6.1.2.1.16.0.2	–	–
Routing Notifications				
BGP 4 MIB	bgpEstablished	1.3.6.1.2.1.15.7.1	–	–
	bgpBackwardTransition	1.3.6.1.2.1.15.7.2	–	–

Copyright © 2018, Juniper Networks, Inc.

Table 42: Standard SNMPv2 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

Defined in	Trap Name	SNMP Trap OID	System Logging Severity Level	Syslog Tag
OSPF Trap MIB	ospfVirtIfStateChange	1.3.6.1.2.1.14.16.2.1	–	–
	ospfNbrStateChange	1.3.6.1.2.1.14.16.2.2	–	–
	ospfVirtNbrStateChange	1.3.6.1.2.1.14.16.2.3	–	–
	ospfIfConfigError	1.3.6.1.2.1.14.16.2.4	–	–
	ospfVirtIfConfigError	1.3.6.1.2.1.14.16.2.5	–	–
	ospfIfAuthFailure	1.3.6.1.2.1.14.16.2.6	–	–
	ospfVirtIfAuthFailure	1.3.6.1.2.1.14.16.2.7	–	–
	ospfIfRxBadPacket	1.3.6.1.2.1.14.16.2.8	–	–
	ospfVirtIfRxBadPacket	1.3.6.1.2.1.14.16.2.9	–	–
	ospfTxRetransmit	1.3.6.1.2.1.14.16.2.10	–	–
	ospfVirtIfTxRetransmit	1.3.6.1.2.1.14.16.2.11	–	–
	ospfMaxAgeLsa	1.3.6.1.2.1.14.16.2.13	–	–
	ospfIfStateChange	1.3.6.1.2.1.14.16.2.16	–	–
Startup Notifications				
RFC 1907, *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)*	coldStart	1.3.6.1.6.3.1.1.5.1	Critical	SNMPD_TRAP_ COLD_START
	warmStart	1.3.6.1.6.3.1.1.5.2	Error	SNMPD_TRAP_ WARM_START
	authenticationFailure	1.3.6.1.6.3.1.1.5.5	Notice	SNMPD_TRAP_ GEN_FAILURE
VRRP Notifications				
RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol*	vrrpTrapNewMaster	1.3.6.1.2.1.68.0.1	Warning	VRRPD_NEWMASTER_ TRAP
	vrrpTrapAuthFailure	1.3.6.1.2.1.68.0.2	Warning	VRRPD_AUTH_ FAILURE_ TRAP

Copyright © 2018, Juniper Networks, Inc.

Table 43: Enterprise-Specific SNMPv2 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis

Source MIB	Trap Name	SNMP Trap OID	System Logging Severity Level	System Log Tag
Chassis (Alarm Conditions) Notifications				
Chassis MIB (mib-jnx-chassis)	jnxPowerSupplyFailure	1.3.6.1.4.1.2636.4.1.1	Alert	CHASSISD_ SNMP_ TRAP
	jnxFanFailure	1.3.6.1.4.1.2636.4.1.2	Critical	CHASSISD_ SNMP_ TRAP
	jnxOverTemperature	1.3.6.1.4.1.2636.4.1.3	Critical	CHASSISD_ SNMP_ TRAP
	jnxFruRemoval	1.3.6.1.4.1.2636.4.1.5	Notice	CHASSISD_ SNMP_ TRAP
	jnxFruInsertion	1.3.6.1.4.1.2636.4.1.6	Notice	CHASSISD_ SNMP_ TRAP
	jnxFruPowerOff	1.3.6.1.4.1.2636.4.1.7	Notice	CHASSISD_ SNMP_ TRAP
	jnxFruPowerOn	1.3.6.1.4.1.2636.4.1.8	Notice	CHASSISD_ SNMP_ TRAP
	jnxFruFailed	1.3.6.1.4.1.2636.4.1.9	Warning	CHASSISD_ SNMP_ TRAP
	jnxFruOffline	1.3.6.1.4.1.2636.4.1.10	Notice	CHASSISD_ SNMP_ TRAP
	jnxFruOnline	1.3.6.1.4.1.2636.4.1.11	Notice	CHASSISD_ SNMP_ TRAP
	jnxFruCheck	1.3.6.1.4.1.2636.4.1.12	Notice	CHASSISD_ SNMP_ TRAP
	jnxPowerSupplyOK	1.3.6.1.4.1.2636.4.2.1	Critical	CHASSISD_ SNMP_ TRAP
	jnxFanOK	1.3.6.1.4.1.2636.4.2.2	Critical	CHASSISD_ SNMP_ TRAP
	jnxTemperatureOK	1.3.6.1.4.1.2636.4.2.3	Alert	CHASSISD_ SNMP_ TRAP
Configuration Notifications				

Table 43: Enterprise-Specific SNMPv2 Traps Supported on QFX Series Standalone Switches and QFX Series Virtual Chassis *(continued)*

Source MIB	Trap Name	SNMP Trap OID	System Logging Severity Level	System Log Tag
Configuration Management MIB (mib-jnx-cfgmgmt)	jnxCmCfgChange	1.3.6.1.4.1.2636.4.5.0.1	–	–
	jnxCmRescueChange	1.3.6.1.4.1.2636.4.5.0.2	–	–
Remote Operations Notifications				
Ping MIB (mib-jnx-ping)	jnxPingRttThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.1	–	–
	jnxPingRttStdDevThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.2	–	–
	jnxPingRttJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.3	–	–
	jnxPingEgressThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.4	–	–
	jnxPingEgressStdDevThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.5	–	–
	jnxPingEgressJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.6	–	–
	jnxPingIngressThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.7	–	–
	jnxPingIngressStddevThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.8	–	–
	jnxPingIngressJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.9	–	–
RMON Alarms				
RMON MIB (mib-jnx-rmon)	jnxRmonAlarmGetFailure	1.3.6.1.4.1.2636.4. 3.0.1	–	–
	jnxRmonGetOk	1.3.6.1.4.1.2636.4. 3.0.2	–	–

SNMP Traps Supported on QFabric Systems

QFabric systems support standard SNMPv2 traps and Juniper Networks enterprise-specific SNMPv2 traps.

Copyright © 2018, Juniper Networks, Inc.

NOTE: QFabric systems do not support SNMPv1 traps.

For more information, see:

- Table 44 on page 245 for standard SNMPv2 traps
- Table 45 on page 246 for Juniper Networks enterprise-specific SNMPv2 traps

Table 44: Standard SNMPv2 Traps Supported on QFabric Systems

Defined in	Trap Name	SNMP Trap OID	System Logging Severity Level	Syslog Tag
Link Notifications				
RFC 2863, *The Interfaces Group MIB*	linkDown	1.3.6.1.6.3.1.1.5.3	Warning	SNMP_TRAP_ LINK_DOWN
	linkUp	1.3.6.1.6.3.1.1.5.4	Info	SNMP_TRAP_ LINK_UP
Startup Notifications				
RFC 1907, *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)*	coldStart	1.3.6.1.6.3.1.1.5.1	Critical	SNMPD_TRAP_ COLD_START
	warmStart	1.3.6.1.6.3.1.1.5.2	Error	SNMPD_TRAP_ WARM_START
	authenticationFailure	1.3.6.1.6.3.1.1.5.5	Notice	SNMPD_TRAP_ GEN_FAILURE

Copyright © 2018, Juniper Networks, Inc.

Table 45: Enterprise-Specific SNMPv2 Traps Supported on QFabric Systems

Source MIB	Trap Name	SNMP Trap OID	System Logging Severity Level	System Log Tag
Fabric Chassis MIB (mib-jnx-fabric-chassis)	**Fabric Chassis (Alarm Conditions) Notifications**			
	jnxFabricPowerSupplyFailure	1.3.6.1.4.1.2636.4.19.1	Warning	–
	jnxFabricFanFailure	1.3.6.1.4.1.2636.4.19.2	Critical	–
	jnxFabricOverTemperature	1.3.6.1.4.1.2636.4.19.3	Alert	–
	jnxFabricRedundancySwitchover	1.3.6.1.4.1.2636.4.19.4	Notice	–
	jnxFabricFruRemoval	1.3.6.1.4.1.2636.4.19.5	Notice	–
	jnxFabricFruInsertion	1.3.6.1.4.1.2636.4.19.6	Notice	–
	jnxFabricFruPowerOff	1.3.6.1.4.1.2636.4.19.7	Notice	–
	jnxFabricFruPowerOn	1.3.6.1.4.1.2636.4.19.8	Notice	–
	jnxFabricFruFailed	1.3.6.1.4.1.2636.4.19.9	Warning	–
	jnxFabricFruOffline	1.3.6.1.4.1.2636.4.19.10	Notice	–
	jnxFabricFruOnline	1.3.6.1.4.1.2636.4.19.11	Notice	–
	jnxFabricFruCheck	1.3.6.1.4.1.2636.4.19.12	Warning	–
	jnxFabricFEBSwitchover	1.3.6.1.4.1.2636.4.19.13	Warning	–
	jnxFabricHardDiskFailed	1.3.6.1.4.1.2636.4.19.14	Warning	–
	jnxFabricHardDiskMissing	1.3.6.1.4.1.2636.4.19.15	Warning	–
	jnxFabricBootFromBackup	1.3.6.1.4.1.2636.4.19.16	Warning	–
	Fabric Chassis (Alarm Cleared Conditions) Notifications			
	jnxFabricPowerSupplyOK	1.3.6.1.4.1.2636.4.20.1	Critical	–
	jnxFabricFanOK	1.3.6.1.4.1.2636.4.20.2	Critical	–
	jnxFabricTemperatureOK	1.3.6.1.4.1.2636.4.20.3	Alert	–
	jnxFabricFruOK	1.3.6.1.4.1.2636.4.20.4	–	–

Copyright © 2018, Juniper Networks, Inc.

Table 45: Enterprise-Specific SNMPv2 Traps Supported on QFabric Systems *(continued)*

Source MIB	Trap Name	SNMP Trap OID	System Logging Severity Level	System Log Tag
QFabric MIB (mib-jnx-qf-smi)	QFabric MIB Notifications			
	jnxQFabricDownloadIssued	1.3.6.1.4.1.2636.3.42.1.0.1	–	–
	jnxQFabricDownloadFailed	1.3.6.1.4.1.2636.3.42.1.0.2	–	–
	jnxQFabricDownloadSucceeded	1.3.6.1.4.1.2636.3.42.1.0.3	–	–
	jnxQFabricUpgradeIssued	1.3.6.1.4.1.2636.3.42.1.0.4	–	–
	jnxQFabricUpgradeFailed	1.3.6.1.4.1.2636.3.42.1.0.5	–	–
	jnxQFabricUpgradeSucceeded	1.3.6.1.4.1.2636.3.42.1.0.6	–	–
Configuration Notifications				
Configuration Management MIB (mib-jnx-cfgmgmt)	jnxCmCfgChange	1.3.6.1.4.1.2636.4.5.0.1	–	–
	jnxCmRescueChange	1.3.6.1.4.1.2636.4.5.0.2	–	–
Remote Operations Notifications				
Ping MIB (mib-jnx-ping)	jnxPingRttThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.1	–	–
	jnxPingRttStdDevThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.2	–	–
	jnxPingRttJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.3	–	–
	jnxPingEgressThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.4	–	–
	jnxPingEgressStdDevThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.5	–	–
	jnxPingEgressJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.6	–	–
	jnxPingIngressThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.7	–	–
	jnxPingIngressStddevThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.8	–	–
	jnxPingIngressJitterThreshold Exceeded	1.3.6.1.4.1.2636.4.9.0.9	–	–

Copyright © 2018, Juniper Networks, Inc.

Related Documentation

- SNMP MIB Explorer
- Understanding the Implementation of SNMP on page 212
- *Understanding the Implementation of SNMP on the QFabric System*
- SNMP MIBs Support on page 223

Juniper Networks Enterprise-Specific MIBs

Juniper Networks enterprise-specific MIBs are supported on QFX3500 and QFX3600 switches, and QFabric systems.

NOTE: For information about enterprise-specific SNMP MIB objects, see the SNMP MIB Explorer. You can use SNMP MIB Explorer to view information about various MIBs, MIB objects, and SNMP notifications supported on Juniper Networks devices

For more information, see:

- Table 37 on page 229 for Juniper Networks enterprise-specific MIBs supported on QFX3500 and QFX3600 switches.
- Table 39 on page 234 for Juniper Networks enterprise-specific MIBs supported on QFabric systems.

Table 46: Juniper Networks Enterprise-Specific MIBs Supported on QFX3500 and QFX3600 Switches

MIB	Description
Alarm MIB (mib-jnx-chassis-alarm)	Provides support for alarms from the switch.
Analyzer MIB (mib-jnx-analyzer)	Contains analyzer and remote analyzer data related to port mirroring.
Chassis MIB (mib-jnx-chassis)	Provides support for environmental monitoring (power supply state, board voltages, fans, temperatures, and airflow) and inventory support for the chassis, Flexible PIC Concentrators (FPCs), and PICs.
Chassis Definitions for Router Model MIB (mib-jnx-chas-defines)	Contains the object identifiers (OIDs) that are used by the Chassis MIB to identify routing and switching platforms and chassis components. The Chassis MIB provides information that changes often, whereas the Chassis Definitions for Router Model MIB provides information that changes less often.
Class-of-Service MIB (mib-jnx-cos)	Provides support for monitoring interface output queue statistics per interface and per forwarding class.

Copyright © 2018, Juniper Networks, Inc.

Table 46: Juniper Networks Enterprise-Specific MIBs Supported on QFX3500 and QFX3600 Switches *(continued)*

MIB	Description
Configuration Management MIB (mib-jnx-cfgmgmt)	Provides notification for configuration changes and rescue configuration changes in the form of SNMP traps. Each trap contains the time at which the configuration change was committed, the name of the user who made the change, and the method by which the change was made. A history of the last 32 configuration changes is kept in jnxCmChgEventTable.
Ethernet MAC MIB (mib-jnx-mac)	Monitors media access control (MAC) statistics on Gigabit Ethernet intelligent queuing (IQ) interfaces. It collects MAC statistics; for example, inoctets, inframes, outoctets, and outframes on each source MAC address and virtual LAN (VLAN) ID for each Ethernet port.
Event MIB (mib-jnx-event)	Defines a generic trap that can be generated using an operations script or event policy. This MIB provides the ability to specify a system log string and raise a trap if that system log string is found.
Firewall MIB (mib-jnx-firewall)	Provides support for monitoring firewall filter counters.
Host Resources MIB (mib-jnx-hostresources)	Extends the hrStorageTable object, providing a measure of the usage of each file system on the switch as a percentage. Previously, the objects in the hrStorageTable measured the usage in allocation units—hrStorageUsed and hrStorageAllocationUnits—only. Using the percentage measurement, you can more easily monitor and apply thresholds on usage.
Interface MIB (Extensions) (mib-jnx-if-extensions)	Extends the standard ifTable (RFC 2863) with additional statistics and Juniper Networks enterprise-specific chassis information in the ifJnxTable and ifChassisTable tables.
Ping MIB (mib-jnx-ping)	Extends the standard Ping MIB control table (RFC 2925). Items in this MIB are created when entries are created in pingCtlTable of the Ping MIB. Each item is indexed exactly as it is in the Ping MIB.
RMON Events and Alarms MIB (mib-jnx-rmon)	Supports Junos OS extensions to the standard Remote Monitoring (RMON) Events and Alarms MIB (RFC 2819). The extension augments the alarmTable object with additional information about each alarm. Two additional traps are also defined to indicate when problems are encountered with an alarm.
Structure of Management Information MIB (mib-jnx-smi)	Explains how the Juniper Networks enterprise-specific MIBs are structured.
System Log MIB (mib-jnx-syslog)	Enables notification of an SNMP trap-based application when an important system log message occurs.
Utility MIB (mib-jnx-util)	Provides you with SNMP MIB container objects of the following types: 32-bit counters, 64-bit counters, signed integers, unsigned integers, and octet strings. You can use these objects to store data that can be retrieved using other SNMP operations.
VLAN MIB (mib-jnx-vlan)	Contains information about prestandard IEEE 802.10 VLANs and their association with LAN emulation clients.

Copyright © 2018, Juniper Networks, Inc.

Table 47: Juniper Networks Enterprise-Specific MIBs Supported on QFabric Systems

MIB	Description
Analyzer MIB (mib-jnx-analyzer)	Contains analyzer and remote analyzer data related to port mirroring. The QFabric system supports: • Analyzer table—jnxAnalyzerName, jnxMirroringRatio, jnxLossPriority. • Analyzer input table—jnxAnalyzerInputValue, jnxAnalyzerInputOption, jnxAnalyzerInputType. • , Analyzer output table—jnx AnalyzerOutputValue, jnxAnalyzerOutputType.
Chassis MIB (mib-jnx-chassis)	NOTE: The Chassis MIB has been deprecated for the QFabric system. We recommend that you use the Fabric Chassis MIB (mib-jnx-fabric-chassis) for information about the QFabric system. Provides support for environmental monitoring (power supply state, board voltages, fans, temperatures, and airflow) and inventory support for the chassis, Flexible PIC Concentrators (FPCs), and PICs. NOTE: On the QFabric system, support for scalar variables (such as memory usage) for the Chassis MIB is limited to the following objects: jnxBoxClass, jnxBoxDescr, and jnxBoxSerialNo.
Class-of-Service MIB (mib-jnx-cos)	Provides support for monitoring interface output queue statistics per interface and per forwarding class. The QFabric system supports the following tables and objects: • Jnxcosifstatflagtable—jnxCosIfstatFlags and jnxCosIfIndex. • Jnxcosqstattable—jnxCosQstatTxedPkts, jnxCosQstatTxedPktRate, jnxCosQstatTxedBytes, and jnxCosQstatTxedByteRate. • Jnxcosfcidtable—jnxCosFcIdToFcName. • Jnxcosfctable—jnxCosFcQueueNr. The QFabric system does not support any traps for this MIB.
Configuration Management MIB (mib-jnx-cfgmgmt)	Provides notification for configuration changes and rescue configuration changes in the form of SNMP traps. Each trap contains the time at which the configuration change was committed, the name of the user who made the change, and the method by which the change was made. A history of the last 32 configuration changes is kept in jnxCmChgEventTable. NOTE: On the QFabric system, these conditions apply: • All scalar variables under the jnxCmCfgChg table are supported. • Supported scalar OIDs are jnxCmCfgChgLatestIndex, jnxCmCfgChgLatestTime, jnxCmCfgChgLatestDate, jnxCmCfgChgLatestSource, jnxCmCfgChgLatestUser, and jnxCmCfgChgMaxEventEntries. • Scalar variables under the jnxCmRescueChg table are not supported.
Fabric Chassis MIB (mib-jnx-fabric-chassis)	Provides hardware information about the QFabric system and its component devices. This MIB is based on the Juniper Networks enterprise-specific Chassis MIB but adds another level of indexing that provides information for QFabric system component devices.

Copyright © 2018, Juniper Networks, Inc.

Table 47: Juniper Networks Enterprise-Specific MIBs Supported on QFabric Systems *(continued)*

MIB	Description
Host Resources MIB (mib-jnx-hostresources)	Extends the hrStorageTable object, providing a measure of the usage of each file system on the switch as a percentage. Previously, the objects in the hrStorageTable measured the usage in allocation units—hrStorageUsed and hrStorageAllocationUnits—only. Using the percentage measurement, you can more easily monitor and apply thresholds on usage.
Interface MIB (Extensions) (mib-jnx-if-extensions)	Extends the standard ifTable (RFC 2863) with additional statistics and Juniper Networks enterprise-specific chassis information in the ifJnxTable and ifChassisTable tables. NOTE: On the QFabric system, scalar variables are not supported.
Power Supply Unit MIB (mib-jnx-power-supply-unit)	Provides support for environmental monitoring of the power supply unit for the Interconnect device of the QFabric system. NOTE: On the QFabric system, scalar variables for the jnxPsuObjects 1 object ID in the jnxPsuScalars table are not supported.
QFabric MIB (jnx-qf-smi)	Explains how the Juniper Networks enterprise-specific QFabric MIBs are structured. Defines the MIB objects that are reported by the QFabric system and the contents of the traps that can be issued by the QFabric system.
Utility MIB (mib-jnx-util)	Provides you with SNMP MIB container objects of the following types: 32-bit counters, 64-bit counters, signed integers, unsigned integers, and octet strings. You can use these objects to store data that can be retrieved using other SNMP operations. For more information, see "Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage" on page 277.

Related Documentation

- SNMP MIBs Support on page 223

MIB Objects for the QFX Series

This topic lists the Juniper Networks enterprise-specific SNMP Chassis MIB definition objects for the QFX Series:

- QFX Series Standalone Switches on page 251
- QFabric Systems on page 252
- QFabric System QFX3100 Director Device on page 252
- QFabric System QFX3008-I Interconnect Device on page 252
- QFabric System QFX3600-I Interconnect Device on page 253
- QFabric System Node Devices on page 253

QFX Series Standalone Switches

```
jnxProductLineQFXSwitch       OBJECT IDENTIFIER ::= { jnxProductLine      82 }
  jnxProductNameQFXSwitch       OBJECT IDENTIFIER ::= { jnxProductName      82 }
  jnxProductModelQFXSwitch      OBJECT IDENTIFIER ::= { jnxProductModel     82 }
  jnxProductVariationQFXSwitch  OBJECT IDENTIFIER ::= { jnxProductVariation 82 }
    jnxProductQFX3500s          OBJECT IDENTIFIER ::= { jnxProductVariationQFXSwitch 1 }
```

```
    jnxProductQFX360016QS       OBJECT IDENTIFIER ::= { jnxProductVariationQFXSwitch 2 }
    jnxProductQFX350048T4QS     OBJECT IDENTIFIER ::= { jnxProductVariationQFXSwitch 3 }
    jnxProductQFX510024Q        OBJECT IDENTIFIER ::= { jnxProductVariationQFXSwitch 4 }
    jnxProductQFX510048S6Q      OBJECT IDENTIFIER ::= { jnxProductVariationQFXSwitch 5 }

  jnxChassisQFXSwitch           OBJECT IDENTIFIER ::= { jnxChassis          82 }

  jnxSlotQFXSwitch              OBJECT IDENTIFIER ::= { jnxSlot             82 }
    jnxQFXSwitchSlotFPC         OBJECT IDENTIFIER ::= { jnxSlotQFXSwitch   1 }
    jnxQFXSwitchSlotHM          OBJECT IDENTIFIER ::= { jnxSlotQFXSwitch   2 }
    jnxQFXSwitchSlotPower       OBJECT IDENTIFIER ::= { jnxSlotQFXSwitch   3 }
    jnxQFXSwitchSlotFan         OBJECT IDENTIFIER ::= { jnxSlotQFXSwitch   4 }
    jnxQFXSwitchSlotFPB         OBJECT IDENTIFIER ::= { jnxSlotQFXSwitch   5 }

  jnxMediaCardSpaceQFXSwitch    OBJECT IDENTIFIER ::= { jnxMediaCardSpace   82 }
    jnxQFXSwitchMediaCardSpacePIC OBJECT IDENTIFIER ::= { jnxMediaCardSpaceQFXSwitch 1 }
```

QFabric Systems

```
jnxProductLineQFX3000        OBJECT IDENTIFIER ::= { jnxProductLine 84 }
  jnxProductNameQFX3000         OBJECT IDENTIFIER ::= { jnxProductName 84 }
  jnxProductModelQFX3000        OBJECT IDENTIFIER ::= { jnxProductModel 84 }
  jnxProductVariationQFX3000    OBJECT IDENTIFIER ::= { jnxProductVariation 84 }
   jnxProductQFX3000-G          OBJECT IDENTIFIER ::= { jnxProductVariationQFX3000 1 }
   jnxProductQFX3000-M          OBJECT IDENTIFIER ::= { jnxProductVariationQFX3000 2 }
  jnxChassisQFX3000             OBJECT IDENTIFIER ::= { jnxChassis          84 }
```

QFabric System QFX3100 Director Device

```
jnxProductLineQFX3100 OBJECT IDENTIFIER ::= { jnxProductLine      100 }
  jnxProductNameQFX3100 OBJECT IDENTIFIER ::= { jnxProductName      100 }
  jnxProductModelQFX3100 OBJECT IDENTIFIER ::= { jnxProductModel     100 }
  jnxProductVariationQFX3100  OBJECT IDENTIFIER ::= { jnxProductVariation 100 }
  jnxChassisQFX3100     OBJECT IDENTIFIER ::= { jnxChassis          100 }

  jnxSlotQFX3100            OBJECT IDENTIFIER ::= { jnxSlot             100 }
    jnxQFX3100SlotCPU       OBJECT IDENTIFIER ::= { jnxSlotQFX3100   1 }
    jnxQFX3100SlotMemory    OBJECT IDENTIFIER ::= { jnxSlotQFX3100   2 }
    jnxQFX3100SlotPower     OBJECT IDENTIFIER ::= { jnxSlotQFX3100   3 }
    jnxQFX3100SlotFan       OBJECT IDENTIFIER ::= { jnxSlotQFX3100   4 }
    jnxQFX3100SlotHardDisk  OBJECT IDENTIFIER ::= { jnxSlotQFX3100   5 }
    jnxQFX3100SlotNIC       OBJECT IDENTIFIER ::= { jnxSlotQFX3100   6 }
```

QFabric System QFX3008-I Interconnect Device

```
jnxProductLineQFXInterconnect OBJECT IDENTIFIER ::= { jnxProductLine      60 }
  jnxProductNameQFXInterconnect OBJECT IDENTIFIER ::= { jnxProductName      60 }
  jnxProductModelQFXInterconnect OBJECT IDENTIFIER ::= { jnxProductModel     60 }
  jnxProductVariationQFXInterconnect  OBJECT IDENTIFIER ::= { jnxProductVariation 60 }
    jnxProductQFX3008           OBJECT IDENTIFIER ::= { jnxProductVariationQFXInterconnect 1 }
jnxProductQFXC083008        OBJECT IDENTIFIER ::= { jnxProductVariationQFXInterconnect 2 }
    jnxProductQFX3008I          OBJECT IDENTIFIER ::= { jnxProductVariationQFXInterconnect 3 }

  jnxChassisQFXInterconnect     OBJECT IDENTIFIER ::= { jnxChassis          60 }

  jnxSlotQFXInterconnect        OBJECT IDENTIFIER ::= { jnxSlot             60 }
    jnxQFXInterconnectSlotFPC   OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect   1 }
    jnxQFXInterconnectSlotHM    OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect   2 }
```


Copyright © 2018, Juniper Networks, Inc.

```
    jnxQFXInterconnectSlotPower OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect   3 }
    jnxQFXInterconnectSlotFan   OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect   4 }
    jnxQFXInterconnectSlotCBD   OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect   5 }
    jnxQFXInterconnectSlotFPB   OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect   6 }

  jnxMediaCardSpaceQFXInterconnect    OBJECT IDENTIFIER ::= { jnxMediaCardSpace   60 }
    jnxQFXInterconnectMediaCardSpacePIC OBJECT IDENTIFIER ::= { jnxMediaCardSpaceQFXInterconnect 1 }

  jnxMidplaneQFXInterconnect    OBJECT IDENTIFIER ::= { jnxBackplane        60 }
```

QFabric System QFX3600-I Interconnect Device

```
jnxProductLineQFXMInterconnect OBJECT IDENTIFIER ::= { jnxProductLine      91 }
  jnxProductNameQFXMInterconnect OBJECT IDENTIFIER ::= { jnxProductName      91 }
  jnxProductModelQFXMInterconnect OBJECT IDENTIFIER ::= { jnxProductModel     91 }
  jnxProductVariationQFXMInterconnect  OBJECT IDENTIFIER ::= { jnxProductVariation 91 }
    jnxProductQFX3600I          OBJECT IDENTIFIER ::= { jnxProductVariationQFXMInterconnect 1 }

  jnxChassisQFXMInterconnect     OBJECT IDENTIFIER ::= { jnxChassis          91 }

  jnxSlotQFXMInterconnect        OBJECT IDENTIFIER ::= { jnxSlot             91 }
    jnxQFXMInterconnectSlotFPC   OBJECT IDENTIFIER ::= { jnxSlotQFXMInterconnect   1 }
    jnxQFXMInterconnectSlotHM    OBJECT IDENTIFIER ::= { jnxSlotQFXMInterconnect   2 }
    jnxQFXMInterconnectSlotPower OBJECT IDENTIFIER ::= { jnxSlotQFXMInterconnect   3 }
    jnxQFXMInterconnectSlotFan   OBJECT IDENTIFIER ::= { jnxSlotQFXMInterconnect   4 }
    jnxQFXMInterconnectSlotFPB   OBJECT IDENTIFIER ::= { jnxSlotQFXMInterconnect   5 }

  jnxMediaCardSpaceQFXMInterconnect    OBJECT IDENTIFIER ::= { jnxMediaCardSpace   91 }
    jnxQFXMInterconnectMediaCardSpacePIC OBJECT IDENTIFIER ::= { jnxMediaCardSpaceQFXMInterconnect 1 }
```

QFabric System Node Devices

```
jnxProductLineQFXNode       OBJECT IDENTIFIER ::= { jnxProductLine      61 }
  jnxProductNameQFXNode       OBJECT IDENTIFIER ::= { jnxProductName      61 }
  jnxProductModelQFXNode      OBJECT IDENTIFIER ::= { jnxProductModel     61 }
  jnxProductVariationQFXNode  OBJECT IDENTIFIER ::= { jnxProductVariation 61 }
    jnxProductQFX3500         OBJECT IDENTIFIER ::= { jnxProductVariationQFXNode 1 }
    jnxProductQFX360016Q      OBJECT IDENTIFIER ::= { jnxProductVariationQFXNode 3 }

  jnxChassisQFXNode           OBJECT IDENTIFIER ::= { jnxChassis          61 }

  jnxSlotQFXNode              OBJECT IDENTIFIER ::= { jnxSlot             61 }
    jnxQFXNodeSlotFPC         OBJECT IDENTIFIER ::= { jnxSlotQFXNode   1 }
    jnxQFXNodeSlotHM          OBJECT IDENTIFIER ::= { jnxSlotQFXNode   2 }
    jnxQFXNodeSlotPower       OBJECT IDENTIFIER ::= { jnxSlotQFXNode   3 }
    jnxQFXNodeSlotFan         OBJECT IDENTIFIER ::= { jnxSlotQFXNode   4 }
    jnxQFXNodeSlotFPB         OBJECT IDENTIFIER ::= { jnxSlotQFXNode   5 }

  jnxMediaCardSpaceQFXNode    OBJECT IDENTIFIER ::= { jnxMediaCardSpace   61 }
    jnxQFXNodeMediaCardSpacePIC OBJECT IDENTIFIER ::= { jnxMediaCardSpaceQFXNode 1 }
```

Related Documentation

- *Understanding the Implementation of SNMP on the QFabric System*
- *Fabric Chassis MIB*

Configuring SNMP

SNMP is implemented in the Junos OS Software running on the QFX Series and OCX Series products. By default, SNMP is not enabled. To enable SNMP, you must include the SNMP configuration statements at the **[edit]** hierarchy level.

To configure the minimum requirements for SNMP, include the following statements at the **[edit]** hierarchy level of the configuration:

```
[edit]
snmp {
  community public;
}
```

To configure complete SNMP features, include the following statements at the **[edit]** hierarchy level of the configuration:

```
snmp {
  client-list client-list-name {
    ip-addresses;
  }
  community community-name {
    authorization authorization;
    client-list-name client-list-name;
    clients {
      address restrict;
    }
    logical-system logical-system-name {
      routing-instance routing-instance-name {
        clients {
        addresses;
        }
      }
    }
    routing-instance routing-instance-name {
      clients {
      addresses;
      }
    }
    view view-name;
  }
  contact contact;
  description description;
  filter-duplicates;
  filter-interfaces;
  health-monitor {
    falling-threshold integer;
    interval seconds;
    rising-threshold integer;
  }
  interface [ interface-names ];
  location location;
  name name;
  nonvolatile {
```


Copyright © 2018, Juniper Networks, Inc.

```
    commit-delay seconds;
  }
  rmon {
    alarm index {
      description description;
      falling-event-index index;
      falling-threshold integer;
      falling-threshold-interval seconds;
      interval seconds;
      request-type;
      rising-event-index index;
      rising-threshold integer;
      sample-type (absolute-value | delta-value);
      startup-alarm (falling-alarm | rising-alarm | rising-or-falling alarm);
      syslog-subtag syslog-subtag;
      variable oid-variable;
    }
    event index {
      community community-name;
      description description;
      type type;
    }
    history history-index {
      bucket-size number;
      interface interface-name;
      interval seconds;
      owner owner-name;
    }
  }
  traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable> <match
      regular-expression>;
    flag flag;
  }
  trap-group group-name {
    categories {
      category;
    }
    destination-port port-number;
    routing-instance routing-instance-name;
    targets {
      address;
    }
    version (all | v1 | v2);
  }
  trap-options {
    agent-address outgoing-interface;
    source-address address;
  }
  v3 {
    notify name {
      tag tag-name;
      type trap;
    }
    notify-filter profile-name {
      oid object-identifier (include | exclude);
```

```
}
snmp-community community-index {
   community-name community-name;
   security-name security-name;
   tag tag-name;
}
target-address target-address-name {
   address address;
   address-mask address-mask;
   logical-system logical-system;
   port port-number;
   retry-count number;
   routing-instance routing-instance-name;
   tag-list tag-list;
   target-parameters target-parameters-name;
   timeout seconds;
}
target-parameters target-parameters-name {
   notify-filter profile-name;
   parameters {
      message-processing-model (v1 | v2c | V3);
      security-level (authentication | none | privacy);
      security-model (usm | v1 | v2c);
      security-name security-name;
   }
}
usm {
   local-engine {
      user username {
         authentication-sha {
            authentication-password authentication-password;
         }
         authentication-md5 {
            authentication-password authentication-password;
         }
         authentication-none;
         privacy-aes128 {
            privacy-password privacy-password;
         }
         privacy-des {
            privacy-password privacy-password;
         }
         privacy-3des {
            privacy-password privacy-password;
         }
         privacy-none;
      }
   }
   remote-engine engine-id {
      user username {
         authentication-sha {
            authentication-password authentication-password;
         }
         authentication-md5 {
            authentication-password authentication-password;
         }
```


Copyright © 2018, Juniper Networks, Inc.

```
                authentication-none;
                privacy-aes128 {
                  privacy-password privacy-password;
                }
                privacy-des {
                  privacy-password privacy-password;
                }
                privacy-3des {
                  privacy-password privacy-password;
                }
                privacy-none {
                  privacy-password privacy-password;
                }
              }
            }
          }
          vacm {
            access {
              group group-name {
                (default-context-prefix | context-prefix context-prefix) {
                  security-model (any | usm | v1 | v2c) {
                    security-level (authentication | none | privacy) {
                      notify-view view-name;
                      read-view view-name;
                      write-view view-name;
                    }
                  }
                }
              }
            }
            security-to-group {
              security-model (usm | v1 | v2c) {
                security-name security-name {
                  group group-name;
                }
              }
            }
          }
        }
        view view-name {
          oid object-identifier (include | exclude);
        }
      }
```

Related Documentation

- Understanding the Implementation of SNMP on page 212
- snmp on page 355

Configuring the SNMP Community String

The SNMP community string defines the relationship between an SNMP server system and the client systems. This string acts like a password to control the clients' access to the server. To configure a community string in a Junos OS configuration, include the **community** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
community name {
   authorization authorization;
   clients {
      default restrict;
      address restrict;
   }
   view view-name;
}
```

If the community name contains spaces, enclose it in quotation marks (" ").

The default authorization level for a community is **read-only**. To allow **Set** requests within a community, you need to define that community as **authorization read-write**. For **Set** requests, you also need to include the specific MIB objects that are accessible with read-write privileges using the **view** statement. The default view includes all supported MIB objects that are accessible with read-only privileges; no MIB objects are accessible with read-write privileges. For more information about the **view** statement, see "Configuring MIB Views" on page 261.

The **clients** statement lists the IP addresses of the clients (community members) that are allowed to use this community. If no **clients** statement is present, all clients are allowed. For ***address***, you must specify an IPv4 address, not a hostname. Include the **default restrict** option to deny access to all SNMP clients for which access is not explicitly granted. We recommend that you always include the **default restrict** option to limit SNMP client access to the local switch.

NOTE: **Community names must be unique within each SNMP system.**

Related Documentation

- Configuring SNMP on page 254

Configuring SNMP Trap Groups

Before any SNMP traps can be sent, you must configure a trap group, the categories of traps the group can receive, and the targets (systems) that will receive the traps. To create and name an SNMP trap group, include the **trap-group** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
trap-group group-name {
   categories {
      category;
   }
   destination-port port-number;
   targets {
      address;
   }
   version (all | v1 | v2);
}
```


Copyright © 2018, Juniper Networks, Inc.

The trap group name can be any string and is embedded in the community name field of the trap. To configure your own trap group port, include the **destination-port** statement. The default destination port is port 162.

For each trap group that you define, you must include the **target** statement to define at least one system as the recipient of the SNMP traps in the trap group. Specify the IPv4 address of each recipient and not its hostname.

Specify the types of traps the trap group can receive in the **categories** statement.

A trap group can receive the following categories of traps:

- **authentication**—Authentication failures
- **chassis**—Chassis or environment notifications
- **configuration**—Configuration notifications
- **link**—Link-related notifications such as up-down transitions
- **remote-operations**—Remote operation notifications
- **startup**—System warm and cold starts

The **version** statement allows you to specify the SNMP version of the traps sent to targets of the trap group. If you specify **v1** only, SNMPv1 traps are sent. If you specify **v2** only, SNMPv2 traps are sent. If you specify **all**, both an SNMPv1 and an SNMPv2 trap are sent for every trap condition. For more information about the **version** statement, see version.

Adding a Group of Clients to an SNMP Community

Junos OS enables you to add one or more groups of clients to an SNMP community. You can include the **client-list-name** ***name*** statement at the **[edit snmp community** ***community-name*****]** hierarchy level to add all the members of the client list or prefix list to an SNMP community.

To define a list of clients, include the **client-list** statement followed by the IP addresses of the clients at the **[edit snmp]** hierarchy level:

```
[edit snmp]
  client-list client-list-name {
  ip-addresses;
}
```

You can configure a prefix list at the **[edit policy options]** hierarchy level. Support for prefix lists in the SNMP community configuration enables you to use a single list to configure the SNMP and routing policies. For more information about the **prefix-list** statement, see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide*.

To add a client list or prefix list to an SNMP community, include the **client-list-name** statement at the **[edit snmp community** ***community-name*****]** hierarchy level:

```
[edit snmp community community-name]
client-list-name client-list-name;
```

NOTE: The client list and prefix list must not have the same name.

The following example shows how to define a client list:

```
[edit]
snmp {
   client-list clentlist1 {
      10.1.1.1/32;
      10.2.2.2/32;
   }
}
```

The following example shows how to add a client list to an SNMP community:

```
[edit]
snmp {
   community community1 {
      authorization read-only;
      client-list-name clientlist1;
   }
}
```

The following example shows how to add a prefix list to an SNMP community:

```
[edit]
policy-options {
   prefix-list prefixlist {
   10.3.3.3/32;
   10.5.5.5/32;
   }
}
snmp {
   community community2 {
   client-list-name prefixlist;
   }
}
```

Related Documentation

- client-list on page 297
- client-list-name on page 297

Configuring the Interfaces on Which SNMP Requests Can Be Accepted

By default, all router or switch interfaces have SNMP access privileges. To limit the access through certain interfaces only, include the **interface** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
interface [ interface-names ];
```

Specify the names of any logical or physical interfaces that should have SNMP access privileges. Any SNMP requests entering the router or switch from interfaces not listed are discarded.

 Copyright © 2018, Juniper Networks, Inc.

Related Documentation

- *Configuring SNMP on a Device Running Junos OS*
- *Configuration Statements at the [edit snmp] Hierarchy Level*
- *Example: Configuring Secured Access List Checking*

Configuring MIB Views

SNMPv3 defines the concept of MIB views in RFC 3415, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*. MIB views provide an agent better control over who can access specific branches and objects within its MIB tree. A view consists of a name and a collection of SNMP object identifiers, which are either explicitly included or excluded. Once defined, a view is then assigned to an SNMPv3 group or SNMPv1/v2c community (or multiple communities), automatically masking which parts of the agent's MIB tree members of the group or community can (or cannot) access.

By default, an SNMP community grants read access and denies write access to all supported MIB objects (even communities configured as **authorization read-write**). To restrict or grant read or write access to a set of MIB objects, you must configure a MIB view and associate the view with a community.

To configure MIB views, include the **view** statement at the **[edit snmp]** hierarchy level:

```
[edit snmp]
view view-name {
   oid object-identifier (include | exclude);
}
```

The **view** statement defines a MIB view and identifies a group of MIB objects. Each MIB object of a view has a common object identifier (OID) prefix. Each object identifier represents a subtree of the MIB object hierarchy. The subtree can be represented either by a sequence of dotted integers (such as **1.3.6.1.2.1.2**) or by its subtree name (such as **interfaces**). A configuration statement uses a view to specify a group of MIB objects on which to define access. You can also use a wildcard character asterisk (*) to include OIDs that match a particular pattern in the SNMP view. To enable a view, you must associate the view with a community.

To remove an OID completely, use the **delete view all oid** ***oid-number*** command but omit the **include** parameter.

```
[edit groups global snmp]
user@host# set view view-name oid object-identifier (include | exclude)
```

The following example creates a MIB view called ping-mib-view. The **oid** statement does not require a dot at the beginning of the object identifier. The **snmp view** statement includes the branch under the object identifier .1.3.6.1.2.1.80. This includes the entire DISMAN-PINGMIB subtree (as defined in RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*), which effectively permits access to any object under that branch.

```
[edit groups global snmp]
user@host# set view ping-mib-view oid 1.3.6.1.2.1.80 include
```

The following example adds a second branch in the same MIB view.

```
[edit groups global snmp]
user@host# set view ping-mib-view oid jnxPingMIB include
```

Assign a MIB view to a community that you want to control.

To associate MIB views with a community, include the **view** statement at the **[edit snmp community *community-name*]** hierarchy level:

```
[edit snmp community community-name]
view view-name;
```

For more information about the Ping MIB, see RFC 2925 and PING MIB.

Related Documentation

- *Configuring SNMP on a Device Running Junos OS*
- *Configuration Statements at the [edit snmp] Hierarchy Level*
- *Configuring Ping Proxy MIB*
- *view (Configuring a MIB View)*
- view (Associating MIB View with a Community) on page 384
- *oid*

Configuring RMON Alarms and Events

The Junos OS supports the *Remote Network Monitoring* (RMON) MIB (RFC 2819), which allows a management device to monitor the values of MIB objects, or variables, against configured thresholds. When the value of a variable crosses a threshold, an alarm and its corresponding event are generated. The event can be logged and can generate an SNMP trap.

To configure RMON alarms and events using the CLI, perform these tasks:

1. Configuring SNMP on page 262
2. Configuring an Event on page 263
3. Configuring an Alarm on page 264

Configuring SNMP

To configure SNMP:

1. Grant read-only access to all SNMP clients:

   ```
   [edit snmp]
   user@switch# set community community-name authorization authorization
   ```

   For example:

   ```
   [edit snmp]
   user@switch# set community public authorization read-only
   ```

 Copyright © 2018, Juniper Networks, Inc.

2. Grant read-write access to the **RMON** and **jnx-rmon** MIBs:

```
[edit snmp]
user@switch# set view view-name oid object-identifier include
user@switch# set view view-name oid object-identifier include
user@switch# set community community-name authorization authorization view view-name
```

For example:

```
[edit snmp]
user@switch# set view rmon-mib-view oid .1.3.6.1.2.1.16 include
user@switch# set view rmon-mib-view oid .1.3.6.1.4.1.2636.13 include
user@switch# set community private authorization read-write view rmon-mib-view
```

OIDs 1.3.6.1.2.1.16 and 1.3.6.1.4.1.2636.13 correspond to the **RMON** and **jnxRmon** MIBs.

3. Configure an SNMP trap group:

```
[edit snmp]
user@switch# set trap-group group-name categories category
user@switch# set trap-group group-name targets address
```

For example:

```
[edit snmp]
user@switch# set trap-group rmon-trap-group categories rmon-alarm
user@switch# set trap-group rmon-trap-group targets 192.168.5.5
```

The trap group **rmon-trap-group** is configured to send RMON traps to 192.168.5.5.

Configuring an Event

To configure an event:

1. Configure an event index, community name, and type:

```
[edit snmp rmon]
user@switch# set event index community community-name  typetype
```

For example:

```
[edit snmp rmon]
user@switch# set event 1 community rmon-trap-group type log-and-trap
```

The event community corresponds to the SNMP trap group and is not the same as an SNMP community. This event generates an SNMP trap and adds an entry to the **logTable** in the RMON MIB.

2. Configure a description for the event:

```
[edit snmp rmon]
user@switch# set event index description description
```

For example:

```
[edit snmp rmon]
user@switch# set event 1 description "rmon event"
```

Configuring an Alarm

To configure an alarm:

1. Configure an alarm index, the variable to monitor, the rising and falling thresholds, and the corresponding rising and falling events:

   ```
   [edit snmp rmon]
   user@switch# set alarm index variable oid-variable falling-threshold integer rising-threshold
   integer rising-event-index index falling-event-index index
   ```

   For example:

   ```
   [edit snmp rmon]
   user@switch# set alarm 5 variable .1.3.6.1.4.1.2636.3.1.13.1.8.9.1.0.0 falling-threshold 75
   rising-threshold 90 rising-event-index 1 falling-event-index 1
   ```

   The variable .1.3.6.1.4.1.2636.3.1.13.1.8.9.1.0.0 corresponds to the **jnxRmon** MIB object **jnxOperatingCPU**, which represents the CPU utilization of the Routing Engine. The falling and rising threshold integers are 75 and 90. The rising and falling events both generate the same event (event index 1).

2. Configure the sample interval and type and the alarm type:

   ```
   [edit snmp rmon]
   user@switch# set alarm index interval seconds sample-type (absolute-value | delta-value)
   startup-alarm (falling-alarm | rising-alarm | rising-or-falling-alarm)
   ```

   For example:

   ```
   [edit snmp rmon]
   user@switch# set alarm 5 interval 30 sample-type absolute-value
   startup-alarm rising-or-falling-alarm
   ```

   The absolute value of the monitored variable is sampled every 30 seconds. The initial alarm can occur because of rising above the rising threshold or falling below the falling threshold.

Related Documentation

- Configuring SNMP on page 254
- Juniper Networks Enterprise-Specific MIBs on page 248
- Monitoring RMON MIB Tables on page 271
- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Understanding RMON on page 217

Copyright © 2018, Juniper Networks, Inc.

Configuring Health Monitoring

This topic describes how to configure the health monitor feature for QFX Series and OCX Series devices.

The health monitor feature extends the SNMP RMON alarm infrastructure to provide predefined monitoring for a selected set of object instances (such as file system usage, CPU usage, and memory usage) and dynamic object instances (such as Junos OS processes).

To configure health monitoring:

1. Configure the health monitor:

   [edit snmp]
   user@switch# **set health-monitor**

2. Configure the falling threshold:

   [edit snmp]
   user@switch# **set health-monitor falling-threshold** ***percentage***

   For example:

   user@switch# **set health-monitor falling-threshold 85**

3. Configure the rising threshold:

   [edit snmp]
   user@switch# **set health-monitor rising-threshold** ***percentage***

   For example:

   user@switch# **set health-monitor rising-threshold 75**

4. Configure the interval:

   [edit snmp]
   user@switch# **set health-monitor interval** ***seconds***

   For example:

   user@switch# **set health-monitor interval 600**

Related Documentation

- Understanding Health Monitoring on page 221
- falling-threshold on page 309
- interval (Health Monitor) on page 319
- rising-threshold (Health Monitor) on page 342

Copyright © 2018, Juniper Networks, Inc.

Creating SNMPv3 Users

For each SNMPv3 user, you can specify the username, authentication type, authentication password, privacy type, and privacy password. After a user enters a password, a key based on the engine ID and password is generated and is written to the configuration file. After the generation of the key, the password is deleted from this configuration file.

NOTE: **You can configure only one encryption type for each SNMPv3 user.**

To create users, include the **user** statement at the **[edit snmp v3 usm local-engine]** hierarchy level:

```
[edit snmp v3 usm local-engine]
user username;
```

username is the name that identifies the SNMPv3 user.

To configure user authentication and encryption, include the following statements at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level:

```
[edit snmp v3 usm local-engine user username]
authentication-md5 {
   authentication-password authentication-password;
}
authentication-sha {
   authentication-password authentication-password;
}
authentication-none;
privacy-aes128 {
   privacy-password privacy-password;
}
privacy-des {
   privacy-password privacy-password;
}
privacy-3des {
   privacy-password privacy-password;
}
privacy-none;
```

Related Documentation

- Minimum SNMPv3 Configuration on a Device Running Junos OS on page 216
- *Example: Creating SNMPv3 Users*
- *Example: SNMPv3 Configuration*

Copyright © 2018, Juniper Networks, Inc.

Configuring Access Privileges for a Group

In SNMPv3, you can configure a group that sets the same access privileges for one or more users. Configuring a group includes defining the security model and security level, and associating one or more MIB view permissions for the group.

NOTE: You must associate at least one MIB view with the group. You can associate multiple MIB views (read, notify, write) to authorize different permissions based on the view. The view name cannot exceed 32 characters.

To configure access privileges for a group:

1. To configure the group:

   [edit snmp v3 vacm access]
   user@switch# **edit group** ***group-name***

2. To configure the context prefix of the SNMP instance for the group:

   [edit snmp v3 vacm access group *group-name*]
   user@switch# **edit (default-context-prefix | context-prefix** ***context-prefix*****)**

   For example, to configure the default context prefix:

   [edit snmp v3 vacm access group *group-name*]
   user@switch# **edit default-context-prefix**

3. To configure the security model:

   [edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*)]
   user@switch# **edit security-model (any | usm | v1 | v2c)**

   For example, to configure the SNMPv3 user-based security model (USM):

   [edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*)]
   user@switch# **edit security-model usm**

4. To configure the security level:

   [edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*) security-model (any | usm | v1 | v2c)]
   user@switch# **edit security-level (authentication | none | privacy)**

   For example, to configure a security level requiring user authentication and encryption:

   [edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*) security-model (any | usm | v1 | v2c)]
   user@switch# **edit security-level privacy**

Copyright © 2018, Juniper Networks, Inc.

NOTE: Access privileges are granted to all packets with a security level equal to or greater than that configured. If you are configuring the SNMPv1 or v2c security model, use **none** as your security level. If you are configuring the SNMPv3 security model (USM), use the **authentication**, **none**, or **privacy** security level.

5. (Optional) To associate a read-only MIB view with an SNMP group:

   [edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]
   user@switch# **edit read-view** ***view-name***

6. (Optional) To associate a MIB view with an SNMP notification permission for an SNMP group:

   [edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]
   user@switch# **edit notify-view** ***view-name***

7. (Optional) To associate a MIB view with write permission for an SNMP group:

   [edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]
   user@switch# **edit write-view** ***view-name***

Related Documentation

- SNMPv3 Overview on page 215
- Minimum SNMPv3 Configuration on a Device Running Junos OS on page 216

Assigning a Security Name to a Group

In SNMPv3, each username is associated with a security name. The security name, together with the SNMP engine ID, is included in SNMP messages to ensure messaging security.

Before you assign a security name to a group, first create the security name. For an SNMPv3 client, the security name is the username configured at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level. For SNMPv1 or v2c clients, the security name is the community string configured at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level.

Assigning a security name to a group includes configuring a security model for the group, assigning the security name to the group, and configuring the group.

Copyright © 2018, Juniper Networks, Inc.

To assign an SNMP security name to a group:

1. To configure a security model for the group:

   [edit snmp v3 vacm security-to-group]
   user@switch# **edit security-model (usm | v1 | v2c)**

   For example, to configure the SNMPv3 user-based security model (USM):

   [edit snmp v3 vacm security-to-group]
   user@switch# **edit security-model usm**

2. To associate the security name with a group:

   [edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c)]
   user@switch# **edit security-name** ***security-name***

3. To configure a group of SNMPv3 security names with the same security policy:

   [edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c) security-name *security-name*]
   user@switch# **edit group** ***group-name***

Related Documentation

- Creating SNMPv3 Users on page 266
- group (Defining Access Privileges for an SNMPv3 Group) on page 313
- security-model (Group) on page 349
- security-name (Community String) on page 351
- security-name (Security Group) on page 352

Configuring SNMPv3 Traps on a Device Running Junos OS

In SNMPv3, you create traps and informs by configuring the **notify**, **target-address**, and **target-parameters** parameters. Traps are unconfirmed notifications, whereas informs are confirmed notifications. This section describes how to configure SNMP traps. For information about configuring SNMP informs, see "Configuring SNMP Informs" on page 270.

The target address defines a management application's address and parameters to be used in sending notifications. Target parameters define the message processing and security parameters that are used in sending notifications to a particular management target. SNMPv3 also lets you define SNMPv1 and SNMPv2c traps.

NOTE: When you configure SNMP traps, make sure your configured access privileges allow the traps to be sent. Access privileges are configured at the **[edit snmp v3 vacm access]** and **[edit snmp v3 vacm security-to-group]** hierarchy levels.

To configure SNMP traps, include the following statements at the **[edit snmp v3]** hierarchy level:

```
[edit snmp v3]
notify name {
   tag tag-name;
   type trap;
}
notify-filter name {
   oid object-identifier (include | exclude);
}
target-address target-address-name {
   address address;
   address-mask address-mask;
   logical-system logical-system;
   port port-number;
   routing-instance instance;
   tag-list tag-list;
   target-parameters target-parameters-name;
}
target-parameters target-parameters-name {
   notify-filter profile-name;
   parameters {
      message-processing-model (v1 | v2c | v3);
      security-level (authentication | none | privacy);
      security-model (usm | v1 | v2c);
      security-name security-name;
   }
}
```

Related Documentation

- *Configuring the SNMPv3 Trap Notification*
- *Configuring the Trap Notification Filter*
- *Configuring the Trap Target Address*
- *Defining and Configuring the Trap Target Parameters*
- Configuring SNMP Informs on page 270
- *Configuring the Remote Engine and Remote User*
- *Configuring the Inform Notification Type and Target Address*

Configuring SNMP Informs

Junos OS supports two types of notifications: traps and informs. With traps, the receiver does not send any acknowledgment when it receives a trap. Therefore, the sender cannot determine if the trap was received. A trap may be lost because a problem occurred during transmission. To increase reliability, an inform is similar to a trap except that the inform is stored and retransmitted at regular intervals until one of these conditions occurs:

- The receiver (target) of the inform returns an acknowledgment to the SNMP agent.

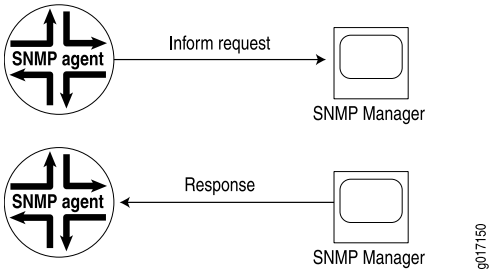
 Copyright © 2018, Juniper Networks, Inc.

- A specified number of unsuccessful retransmissions have been attempted and the agent discards the inform message.

If the sender never receives a response, the inform can be sent again. Thus, informs are more likely to reach their intended destination than traps are. Informs use the same communications channel as traps (same socket and port) but have different protocol data unit (PDU) types.

Informs are more reliable than traps, but they consume more network, router, and switch resources (see Figure 7 on page 271). Unlike a trap, an inform is held in memory until a response is received or the timeout is reached. Also, traps are sent only once, whereas an inform may be retried several times. Use informs when it is important that the SNMP manager receive all notifications. However, if you are more concerned about network traffic, or router and switch memory, use traps.

Figure 7: Inform Request and Response



For information about configuring SNMP traps, see "Configuring SNMPv3 Traps on a Device Running Junos OS" on page 269.

Related Documentation

- Configuring SNMPv3 Traps on a Device Running Junos OS on page 269
- *Configuring the Remote Engine and Remote User*
- *Configuring the Inform Notification Type and Target Address*
- Minimum SNMPv3 Configuration on a Device Running Junos OS on page 216

Monitoring RMON MIB Tables

Purpose Monitor remote monitoring (RMON) alarm, event, and log tables.

Action To display the RMON tables:

```
user@switch> show snmp rmon
Alarm
Index  Variable description                          Value State

     5 monitor
       jnxOperatingCPU.9.1.0.0                           5 falling threshold

Event
Index  Type                        Last Event
    1  log and trap                2010-07-10 11:34:17 PDT
```

```
Event Index: 1
    Description: Event 1 triggered by Alarm 5, rising threshold (90) crossed,
(variable: jnxOperatingCPU.9.1.0.0, value: 100)
    Time: 2010-07-10 11:34:07 PDT
    Description: Event 1 triggered by Alarm 5, falling threshold (75) crossed,
(variable: jnxOperatingCPU.9.1.0.0, value: 5)
    Time: 2010-07-10 11:34:17 PDT
```

Meaning The display shows that an alarm has been defined to monitor jnxRmon MIB object jnxOperatingCPU, which represents the CPU utilization of the Routing Engine. The alarm is configured to generate an event that sends an SNMP trap and adds an entry to the logTable in the RMON MIB. The log table shows that two occurrences of the event have been generated—one for rising above a threshold of 90 percent, and one for falling below a threshold of 75 percent.

Related Documentation

- Configuring RMON Alarms and Events on page 262
- show snmp rmon on page 407
- show snmp rmon history on page 411
- clear snmp statistics on page 387
- clear snmp history on page 386

Monitoring SNMP

There are several commands that you can access in Junos OS operational mode to monitor SNMP information. Some of the commands are:

- **show snmp health-monitor**, which displays the health monitor log and alarm information.
- **show snmp mib**, which displays information from the MIBs, such as device and system information.
- **show snmp statistics**, which displays SNMP statistics such as the number of packets, silent drops, and invalid output values.
- **show snmp rmon**, which displays the RMON alarm, event, history, and log information

The following example provides sample output from the **show snmp health-monitor** command:

```
user@switch> show snmp health-monitor
Alarm
Index  Variable description                          Value State

 32768 Health Monitor: root file system utilization
       jnxHrStoragePercentUsed.1                        58 active

 32769 Health Monitor: /config file system utilization
       jnxHrStoragePercentUsed.2                         0 active
```

 Copyright © 2018, Juniper Networks, Inc.

```
 32770 Health Monitor: RE 0 CPU utilization
       jnxOperatingCPU.9.1.0.0                            0 active

 32773 Health Monitor: RE 0 Memory utilization
       jnxOperatingBuffer.9.1.0.0                        35 active

 32775 Health Monitor: jkernel daemon CPU utilization
       Init daemon                                        0 active
       Chassis daemon                                    50 active
       Firewall daemon                                    0 active
       Interface daemon                                   5 active
       SNMP daemon                                       11 active
       MIB2 daemon                                       42 active
       ...
```

The following example provides sample output from the **show snmp mib** command:

user@switch> show snmp mib walk system

```
sysDescr.0    = Juniper Networks, Inc. qfx3500s internet router, kernel
JUNOS 11.1-20100926.0 #0: 2010-09-26 06:17:38 UTC builder@abc.example.net:
/volume/build/junos/11.1/production/20100926.0/obj-xlr/bsd/sys/compile/JUNIPER-xxxxx

Build date: 2010-09-26 06:00:10 U
sysObjectID.0 = jnxProductQFX3500
sysUpTime.0   = 24444184
sysContact.0  = J Smith
sysName.0     = Lab QFX3500
sysLocation.0 = Lab
sysServices.0 = 4
```

The following example provides sample output from the **show snmp statistics** command:

user@switch> show snmp statistics

```
SNMP statistics:
  Input:
    Packets: 0, Bad versions: 0, Bad community names: 0,
    Bad community uses: 0, ASN parse errors: 0,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 0, Total set varbinds: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
    Throttle drops: 0, Duplicate request drops: 0
    Output:
    Packets: 0, Too bigs: 0, No such names: 0,
    Bad values: 0, General errors: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 0, Traps: 0
```

Related Documentation

- health-monitor on page 315
- show snmp mib on page 404
- show snmp statistics on page 412

Tracing SNMP Activity on a Device Running Junos OS

SNMP tracing operations track activity for SNMP agents and record the information in log files. The logged error descriptions provide detailed information to help you solve problems faster.

By default, Junos OS does not trace any SNMP activity. If you include the **traceoptions** statement at the **[edit snmp]** hierarchy level, the default tracing behavior is:

- Important activities are logged in files located in the **/var/log** directory. Each log is named after the SNMP agent that generates it. Currently, the following log files are created in the **/var/log** directory when the **traceoptions** statement is used:
  - chassisd
  - craftd
  - ilmid
  - mib2d
  - rmopd
  - serviced
  - snmpd
- When a trace file named ***filename*** reaches its maximum size, it is renamed ***filename*.0**, then ***filename*.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. (For more information about how log files are created, see the System Log Explorer.)
- Log files can be accessed only by the user who configured the tracing operation.

You cannot change the directory (**/var/log**) in which trace files are located. However, you can customize the other trace file settings by including the following statements at the **[edit snmp]** hierarchy level:

```
[edit snmp]
traceoptions {
   file <files number> <match regular-expression> <size size> <world-readable |
      no-world-readable>;
   flag flag;
   memory-trace;
   no-remote-trace;
   no-default-memory-trace;
}
```

These statements are described in the following sections:

- Configuring the Number and Size of SNMP Log Files on page 275
- Configuring Access to the Log File on page 275
- Configuring a Regular Expression for Lines to Be Logged on page 275
- Configuring the Trace Operations on page 275

Copyright © 2018, Juniper Networks, Inc.

Configuring the Number and Size of SNMP Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed ***filename*.0**, then ***filename*.1**, and so on, until there are three trace files. Then the oldest trace file (***filename*.2**) is overwritten.

You can configure the limits on the number and size of trace files by including the following statements at the **[edit snmp traceoptions]** hierarchy level:

```
[edit snmp traceoptions]
file files number size size;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation (***filename***) reaches 2 MB, ***filename*** is renamed ***filename*.0**, and a new file called ***filename*** is created. When the new ***filename*** reaches 2 MB, ***filename*.0** is renamed ***filename*.1** and ***filename*** is renamed ***filename*.0**. This process repeats until there are 20 trace files. Then the oldest file (***filename*.19**) is overwritten by the newest file (***filename*.0**).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10 KB through 1 gigabyte (GB).

Configuring Access to the Log File

By default, log files can be accessed only by the user who configured the tracing operation.

To specify that any user can read all log files, include the **file world-readable** statement at the **[edit snmp traceoptions]** hierarchy level:

```
[edit snmp traceoptions]
file world-readable;
```

To explicitly set the default behavior, include the **file no-world-readable** statement at the **[edit snmp traceoptions]** hierarchy level:

```
[edit snmp traceoptions]
file no-world-readable;
```

Configuring a Regular Expression for Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged activities.

You can refine the output by including the **match** statement at the **[edit snmp traceoptions file *filename*]** hierarchy level and specifying a regular expression (regex) to be matched:

```
[edit snmp traceoptions]
file filename match regular-expression;
```

Configuring the Trace Operations

By default, only important activities are logged. You can specify which trace operations are to be logged by including the following **flag** statement (with one or more tracing flags) at the **[edit snmp traceoptions]** hierarchy level:

```
[edit snmp traceoptions]
flag {
```

```
    all;
    configuration;
    database;
    events;
    general;
    interface-stats;
    nonvolatile-sets;
    pdu;
    policy;
    protocol-timeouts;
    routing-socket;
    server;
    subagent;
    timer;
    varbind-error;
}
```

Table 48 on page 276 describes the meaning of the SNMP tracing flags.

Table 48: SNMP Tracing Flags

Flag	Description	Default Setting
all	Log all operations.	Off
configuration	Log reading of the configuration at the **[edit snmp]** hierarchy level.	Off
database	Log events involving storage and retrieval in the events database.	Off
events	Log important events.	Off
general	Log general events.	Off
interface-stats	Log physical and logical interface statistics.	Off
nonvolatile-set	Log nonvolatile SNMP set request handling.	Off
pdu	Log SNMP request and response packets.	Off
policy	Log policy processing.	Off
protocol-timeouts	Log SNMP response timeouts.	Off
routing-socket	Log routing socket calls.	Off
server	Log communication with processes that are generating events.	Off
subagent	Log subagent restarts.	Off
timer	Log internal timer events.	Off

Copyright © 2018, Juniper Networks, Inc.

Table 48: SNMP Tracing Flags *(continued)*

Flag	Description	Default Setting
varbind-error	Log variable binding errors.	Off

To display the end of the log for an agent, issue the **show log *agent*d | last** operational mode command:

```
[edit]
user@host# run show log agentd | last
```

where ***agent*** is the name of an SNMP agent.

Related Documentation

- *Configuring SNMP on a Device Running Junos OS*
- *Configuration Statements at the [edit snmp] Hierarchy Level*
- *Example: Tracing SNMP Activity*
- Configuring SNMP on page 254

Using the Enterprise-Specific Utility MIB to Enhance SNMP Coverage

Even though the Junos OS has built-in performance metrics and monitoring options, you might need to have customized performance metrics. To make it easier for you to monitor such customized data through a standard monitoring system, the Junos OS provides you with an enterprise-specific Utility MIB that can store such data and thus extend SNMP support for managing and monitoring the data of your choice.

The enterprise-specific Utility MIB provides you with container objects of the following types: **32-bit counters**, **64-bit counters**, **signed integers**, **unsigned integers**, and **octet strings**. You can use these container MIB objects to store the data that are otherwise not supported for SNMP operations. You can populate data for these objects either by using CLI commands or with the help of Op scripts and an RPC API that can invoke the CLI commands.

The following CLI commands enable you to set and clear Utility MIB object values:

- **request snmp utility-mib set instance *name* object-type <counter | counter 64 | integer | string | unsigned integer> object-value *value***
- **request snmp utility-mib clear instance *name* object-type <counter | counter 64 | integer | string | unsigned integer>**

The **instance *name*** option of the **request snmp utility-mib <set | clear>** command specifies the name of the data instance and is the main identifier of the data. The **object-type <counter | counter 64 | integer | string | unsigned integer>** option enables you specify the object type, and the **object-value *value*** option enables you to set the value of the object.

To automate the process of populating Utility MIB data, you can use a combination of an event policy and event script. The following examples show the configuration for an

event policy to run **show system buffers** every hour and to store the **show system buffers** data in Utility MIB objects by running an event script (**check-mbufs.slax**).

Event Policy Configuration

To configure an event policy that runs the **show system buffers** command every hour and invokes **check-mbufs.slax** to store the **show system buffers** data into Utility MIB objects, include the following statements at the [**edit**] hierarchy level:

```
event-options {
  generate-event {
    1-HOUR time-interval 3600;
  }
  policy MBUFS {
    events 1-HOUR;
    then {
      event-script check-mbufs.slax; # script stored at /var/db/scripts/event/
    }
  }
  event-script {
    file check-mbufs.slax;
  }
}
```

check-mbufs.slax Script

The following example shows the **check-mbufs.slax** script that is stored under **/var/db/scripts/event/**:

```
------ script START ------
version 1.0;

ns junos = "http://xml.juniper.net/junos/*/junos";
ns xnm = "http://xml.juniper.net/xnm/1.1/xnm";
ns jcs = "http://xml.juniper.net/junos/commit-scripts/1.0";
ns ext = "http://xmlsoft.org/XSLT/namespace";

match / {
    <op-script-results>{
 var $cmd = <command> "show system buffers";
        var $out = jcs:invoke($cmd);

     var $lines = jcs:break_lines($out);
     for-each ($lines) {
         if (contains(., "current/peak/max")) {
             var $pattern = "([0-9]+)/([0-9]+)/([0-9]+) mbufs";
             var $split = jcs:regex($pattern, .);
             var $result = $split[2];

             var $rpc = <request-snmp-utility-mib-set> {
                 <object-type> "integer";
                 <instance> "current-mbufs";
                 <object-value> $result;
             }
             var $res = jcs:invoke($rpc);
                }
        }
    }
}
------ script END ------
```


Copyright © 2018, Juniper Networks, Inc.

You can run the following command to check the data stored in the Utility MIB as a result of the event policy and script shown in the preceding examples:

```
user@host> show snmp mib walk jnxUtilData ascii jnxUtilIntegerValue."current-mbufs"
= 0 jnxUtilIntegerTime."current-mbufs" = 07 da 05 0c 03 14 2c 00 2d 07 00
user@caramels>
```

NOTE: The **show snmp mib walk** command is not available on the QFabric system, but you can use external SNMP client applications to perform this operation.

Related Documentation

- *Understanding SNMP Implementation in Junos OS*
- *Configuring SNMP on Devices Running Junos OS*
- *Monitoring SNMP Activity and Tracking Problems That Affect SNMP Performance on a Device Running Junos OS*
- *Optimizing the Network Management System Configuration for the Best Results*
- *Configuring Options on Managed Devices for Better SNMP Response Time*
- *Managing Traps and Informs*
- *Understanding the Implementation of SNMP on the QFabric System*

Example: Configuring SNMP

By default, SNMP is disabled on devices running Junos OS. This example describes the steps for configuring SNMP on the QFabric system.

- Requirements on page 279
- Overview on page 279
- Configuration on page 280

Requirements

This example uses the following hardware and software components:

- Junos OS Release 12.2
- Network management system (NMS) (running the SNMP manager)
- QFabric system (running the SNMP agent) with multiple Node devices

Overview

Because SNMP is disabled by default on devices running Junos OS, you must enable SNMP on your device by including configuration statements at the **[edit snmp]** hierarchy level. At a minimum, you must configure the **community public** statement. The community defined as public grants read-only access to MIB data to any client.

If no **clients** statement is configured, all clients are allowed. We recommend that you always include the **restrict** option to limit SNMP client access to the switch.

The network topology in this example includes an NMS, a QFabric system with four Node devices, and external SNMP servers that are configured for receiving traps.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set snmp name “snmp qfabric” description “qfabric0 switch”
set snmp location “Lab 4 Row 11” contact “qfabric-admin@qfabric0”
set snmp community public authorization read-only
set snmp client-list list0 192.168.0.0/24
set snmp community public client-list-name list0
set snmp community public clients 192.170.0.0/24 restrict
set snmp trap-group “qf-traps” destination-port 155 targets 192.168.0.100
```

Step-by-Step Procedure

The following example requires that you navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure SNMP on the QFabric system:

NOTE: **If the name, description, location, contact, or community name contains spaces, enclose the text in quotation marks (" ").**

1. Configure the SNMP system name:

   ```
   [edit snmp]
   user@switch# set name “snmp qfabric”
   ```

2. Specify a description.

   ```
   [edit snmp]
   user@switch# set description “qfabric0 system”
   ```

   This string is placed into the MIB II sysDescription object.

3. Specify the physical location of the QFabric system.

   ```
   [edit snmp]
   user@switch# set location “Lab 4 Row 11”
   ```

   This string is placed into the MIB II sysLocation object.

4. Specify an administrative contact for the SNMP system.

Copyright © 2018, Juniper Networks, Inc.

```
[edit snmp]
user@switch# set contact "qfabric-admin@qfabric0"
```

This name is placed into the MIB II sysContact object.

5. Specify a unique SNMP community name and the read-only authorization level.

   NOTE: The read-write option is not supported on the QFabric system.

   ```
   [edit snmp]
   user@switch# set community public authorization read-only
   ```

6. Create a client list with a set of IP addresses that can use the SNMP community.

   ```
   [edit snmp]
   user@switch# set client-list list0 192.168.0.0/24
   user@switch# set community public client-list-name list0
   ```

7. Specify IP addresses of clients that are restricted from using the community.

   ```
   [edit snmp]
   user@switch# set community public clients 198.51.100.0/24 restrict
   ```

8. Configure a trap group, destination port, and a target to receive the SNMP traps in the trap group.

   ```
   [edit snmp]
   user@switch# set trap-group "qf-traps" destination-port 155 targets 192.168.0.100
   ```

   NOTE: You do not need to include the destination-port statement if you use the default port 162.

   The trap group qf-traps is configured to send traps to 192.168.0.100.

Results From configuration mode, confirm your configuration by entering the **show** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@switch# show
  snmp {
    name "snmp qfabric";
    description "qfabric0 system";
    location "Lab 4 Row 11";
    contact "qfabric-admin@qfabric0";
    client-list list0 {
      192.168.0.0/24;
```

```
    }
    community public {
      authorization read-only;
      clients {
        198.51.100.0/24 restrict;
      }
    }
    trap-group qf-traps {
      destination-port 155;
      targets {
        192.168.0.100;
      }
    }
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

Related Documentation

- *Understanding the Implementation of SNMP on the QFabric System*
- snmp on page 355

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 14

SNMP Configuration Statements

- access (SNMP) on page 286
- address (SNMP) on page 287
- address-mask on page 287
- agent-address on page 288
- alarm (SNMP RMON) on page 289
- authentication-md5 on page 290
- authentication-none on page 291
- authentication-password on page 292
- authentication-sha on page 293
- authorization on page 294
- bucket-size on page 295
- categories on page 296
- client-list on page 297
- client-list-name on page 297
- clients on page 298
- commit-delay on page 299
- community (SNMP) on page 300
- community (RMON) on page 301
- community-name on page 302
- contact on page 303
- description on page 303
- description (RMON) on page 304
- destination-port (SNMP) on page 305
- engine-id on page 306
- event on page 307
- falling-event-index (RMON) on page 308
- falling-threshold (Health Monitor) on page 309
- falling-threshold (RMON) on page 310

Copyright © 2018, Juniper Networks, Inc.

- falling-threshold-interval on page 311
- filter-duplicates on page 312
- filter-interfaces on page 312
- group (Defining Access Privileges for an SNMPv3 Group) on page 313
- group (Configuring Group Name) on page 314
- health-monitor on page 315
- history on page 316
- interface (SNMP) on page 317
- interface (RMON) on page 318
- interval (Health Monitor) on page 319
- interval (RMON) on page 320
- local-engine on page 321
- location on page 322
- message-processing-model on page 322
- name on page 323
- nonvolatile on page 323
- notify on page 324
- notify-filter (Applying to the Management Target) on page 325
- notify-filter (Configuring the Profile Name) on page 326
- notify-view on page 327
- oid on page 328
- oid (SNMPv3) on page 329
- owner on page 330
- parameters on page 331
- port on page 332
- privacy-3des on page 333
- privacy-aes128 on page 334
- privacy-des on page 335
- privacy-none on page 335
- privacy-password on page 336
- read-view on page 337
- remote-engine on page 338
- request-type on page 339
- retry-count on page 340
- rising-event-index on page 341
- rising-threshold (Health Monitor) on page 342
- rising-threshold (RMON) on page 343

 Copyright © 2018, Juniper Networks, Inc.

- rmon on page 344
- sample-type on page 345
- security-level (Defining Access Privileges) on page 346
- security-level (Generating SNMP Notifications) on page 347
- security-model (Access Privileges) on page 348
- security-model (Group) on page 349
- security-model (SNMP Notifications) on page 350
- security-name (Community String) on page 351
- security-name (Security Group) on page 352
- security-name (SNMP Notifications) on page 353
- security-to-group on page 354
- snmp on page 355
- snmp-community on page 359
- source-address (SNMP) on page 360
- startup-alarm on page 361
- syslog-subtag on page 362
- tag (Configuring Notification Targets) on page 363
- tag-list on page 364
- target-address on page 365
- target-parameters on page 366
- targets on page 367
- timeout on page 368
- traceoptions (SNMP) on page 369
- trap-group on page 371
- trap-options on page 372
- type (RMON Notification) on page 373
- type on page 374
- user on page 375
- usm on page 376
- v3 on page 378
- vacm on page 380
- variable on page 381
- version on page 382
- view (Configuring a MIB View) on page 383
- view (Associating MIB View with a Community) on page 384
- write-view on page 384

Copyright © 2018, Juniper Networks, Inc.

access (SNMP)

Syntax

```
access {
  group group-name {
    (default-context-prefix | context-prefix context-prefix) {
      security-model (any | usm | v1 | v2c) {
        security-level (authentication | none | privacy) {
          notify-view view-name;
          read-view view-name;
          write-view view-name;
        }
      }
    }
  }
}
```

Hierarchy Level

[edit snmp v3 vacm]

Release Information

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

Set SNMP access limits.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Copyright © 2018, Juniper Networks, Inc.

address (SNMP)

Syntax address *address*;

Hierarchy Level [edit snmp v3 target-address *target-address-name*]

Release Information 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 the SNMP target address for receiving traps or informs.

Options ***address***—IPv4 address of the system to receive traps or informs. You must specify an address, not a hostname.

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

Related Documentation

- *Understanding the Implementation of SNMP on the QFabric System*
- Configuring SNMP on page 254
- Example: Configuring SNMP on page 279

address-mask

Syntax address-mask *address-mask*;

Hierarchy Level [edit snmp v3 target-address *target-address-name*]

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 on the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Verify the source addresses for a group of target addresses.

Options ***address-mask*** combined with the address defines a range of addresses.

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

Related Documentation

- *Configuring the Address Mask*

agent-address

Syntax agent-address outgoing-interface;

Hierarchy Level [edit snmp trap-options]

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

Description Set the agent address of all SNMPv1 traps generated by this router or switch. Currently, the only option is **outgoing-interface**, which sets the agent address of each SNMPv1 trap to the address of the outgoing interface of that trap.

Options **outgoing-interface**—Value of the agent address of all SNMPv1 traps generated by this router or switch. The **outgoing-interface** option sets the agent address of each SNMPv1 trap to the address of the outgoing interface of that trap.

Default: Disabled (the agent address is not specified in SNMPv1 traps).

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

Related Documentation

- *Configuring the Agent Address for SNMP Traps*

 Copyright © 2018, Juniper Networks, Inc.

alarm (SNMP RMON)

Syntax

```
alarm index {
   description description;
   falling-event-index index;
   falling-threshold integer;
   falling-threshold-interval seconds;
   interval seconds;
   request-type (get-next-request | get-request | walk-request);
   rising-event-index index;
   rising-threshold integer;
   sample-type (absolute-value | delta-value);
   startup-alarm (falling-alarm | rising-alarm | rising-or-falling alarm);
   syslog-subtag syslog-subtag;
   variable oid-variable;
}
```

Hierarchy Level

[edit snmp rmon]

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 RMON alarm entries.

Options

index—Identifies this alarm entry as an integer.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring an RMON Alarm Entry and Its Attributes*
- *event*
- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Monitoring RMON MIB Tables on page 271
- Understanding RMON on page 217

authentication-md5

Syntax

```
authentication-md5 {
   (authentication-key authentication-key | authentication-password
      authentication-password);
}
```

Hierarchy Level

[edit snmp v3 usm local-engine user *username*],
[edit snmp v3 usm remote-engine *engine-id* 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.

Description

Configure MD5 as the authentication type for the SNMPv3 user.

NOTE: **You can only configure one authentication type for each SNMPv3 user.**

For authentication, you can either enter a password in clear text, which is immediately encrypted, or, if you already have the encrypted version (known as a *key*), enter the key directly.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring MD5 Authentication*

Copyright © 2018, Juniper Networks, Inc.

authentication-none

Syntax authentication-none;

Hierarchy Level [edit snmp v3 usm local-engine user *username*],
[edit snmp v3 usm remote-engine *engine-id* 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 Configure that there should be no authentication for the SNMPv3 user.

NOTE: **You can configure only one authentication type for each SNMPv3 user.**

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

Related Documentation

- *Configuring No Authentication*

authentication-password

Syntax authentication-password *authentication-password*;

Hierarchy Level [edit snmp v3 usm local-engine user *username* authentication-md5],
[edit snmp v3 usm local-engine user *username* authentication-sha],
[edit snmp v3 usm remote-engine *engine-id* user *username* authentication-md5],
[edit snmp v3 usm remote-engine *engine-id* user *username* authentication-sha]

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 password for user authentication.

Options ***authentication-password***—Password that a user enters. The password is then converted into a key that is used for authentication.

SNMPv3 has special requirements when you create plain-text passwords on a router or switch:

- The password must be at least eight characters long.
- The password can include alphabetic, numeric, and special characters, but it cannot include control characters.

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

Related Documentation
- *Configuring MD5 Authentication*
- *Configuring SHA Authentication*

 Copyright © 2018, Juniper Networks, Inc.

authentication-sha

Syntax

```
authentication-sha {
   (authentication-key authentication-key | authentication-password
      authentication-password);
}
```

Hierarchy Level

[edit snmp v3 usm local-engine user *username*],
[edit snmp v3 usm remote-engine *engine-id* 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.

Description

Configure the secure hash algorithm (SHA) as the authentication type for the SNMPv3 user.

NOTE: **You can configure only one authentication type for each SNMPv3 user.**

For authentication, you can either enter a password in clear text, which is immediately encrypted, or, if you already have the encrypted version (known as a *key*), enter the key directly.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring SHA Authentication*

authorization

Syntax authorization *authorization*;

Hierarchy Level [edit snmp community *community-name*]

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

Description Set the access authorization for SNMP **Get**, **GetBulk**, **GetNext**, and **Set** requests.

Options ***authorization***—Access authorization level:

- **read-only**—Enable **Get**, **GetNext**, and **GetBulk** requests.
- **read-write**—Enable all requests, including **Set** requests. You must configure a view to enable **Set** requests.

NOTE: **The read-write option is not supported on the QFX3000 QFabric system.**

Default: read-only

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

Related Documentation

- Configuring the SNMP Community String on page 257

 Copyright © 2018, Juniper Networks, Inc.

bucket-size

Syntax bucket-size *number*;

Hierarchy Level [edit snmp rmon history *index*]

Release Information 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 sampling of Ethernet statistics for network fault diagnosis, planning, and performance tuning.

Default 50

Options ***number***—Number of discrete samples of Ethernet statistics requested.

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

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Configuring RMON Alarms and Events on page 262
- Monitoring RMON MIB Tables on page 271
- Understanding RMON on page 217
- *Junos OS Network Management Configuration Guide*

categories

Syntax

```
categories {
   category;
}
```

Hierarchy Level

[edit snmp trap-group *group-name*]

Release Information

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

Description

Define the types of traps that are sent to the targets of the named trap group.

Default

If you omit the **categories** statement, all trap types are included in trap notifications.

Options

category—Name of a trap type: **authentication**, **chassis**, **configuration**, **link**, **remote-operations**, **rmon-alarm**, or **startup**.

Required Privilege Level

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

Related Documentation

- Configuring SNMP Trap Groups on page 258

Copyright © 2018, Juniper Networks, Inc.

client-list

Syntax

```
client-list client-list-name {
   ip-addresses;
}
```

Hierarchy Level [edit snmp]

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

Description Define a list of SNMP clients.

Options ***client-list-name***—Name of the client list.

ip-addresses—IP addresses of the SNMP clients to be added to the client list,

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

Related Documentation

- Adding a Group of Clients to an SNMP Community on page 259

client-list-name

Syntax client-list-name *client-list-name*;

Hierarchy Level [edit snmp community *community-name*]

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

Description Add a client list or prefix list to an SNMP community.

Options ***client-list-name***—Name of the client list or prefix list.

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

Related Documentation

- Adding a Group of Clients to an SNMP Community on page 259

clients

Syntax

```
clients {
  address <restrict>;
}
```

Hierarchy Level

[edit snmp community *community-name*]

Release Information

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

Description

Specify the IPv4 or IPv6 addresses of the SNMP client hosts that are authorized to use this community.

Default

If you omit the **clients** statement, all SNMP clients using this community string are authorized to access the switch.

Options

address—Address of an SNMP client that is authorized to access this switch. You must specify an address, not a hostname. To specify more than one client, include multiple ***address*** options.

restrict—(Optional) Do not allow the specified SNMP client to access the switch.

Required Privilege Level

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

Related Documentation

- *Configuring SNMP Communities*

Copyright © 2018, Juniper Networks, Inc.

commit-delay

Syntax commit-delay *seconds*;

Hierarchy Level [edit snmp nonvolatile]

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

Description Configure the timer for the SNMP **Set** reply and start of the commit.

Options ***seconds***—Delay between an affirmative SNMP **Set** reply and start of the commit operation.
Default: 5 seconds

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

Related Documentation
- *Configuring the Commit Delay Timer*

community (SNMP)

Syntax

```
community community-name {
  authorization authorization;
  client-list-name client-list-name;
  clients {
    address restrict;
  }
  view view-name;
}
```

Hierarchy Level

[edit snmp]

Release Information

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

Description

Define an SNMP community. An SNMP community authorizes SNMP clients based on the source IP address of incoming SNMP request packets. A community also defines which MIB objects are available and the operations (read-only or read-write) allowed on those objects.

NOTE: **The authorization read-write option is not supported on the QFX3000 QFabric system.**

The SNMP client application specifies an SNMP community name in **Get**, **GetBulk**, **GetNext**, and **Set** SNMP requests.

Default

If you omit the **community** statement, all SNMP requests are denied.

Options

community-name—Community string. If the name includes spaces, enclose it in quotation marks (" ").

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Configuring the SNMP Community String on page 257

Copyright © 2018, Juniper Networks, Inc.

community (RMON)

Syntax community *community-name*;

Hierarchy Level [edit snmp rmon event *index*]

Release Information 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 SNMP trap group that is used when generating a trap (if the eventType object is configured to send traps). If that trap group has the rmon-alarm trap category configured, a trap is sent to all the targets configured for that trap group. The community string in the trap matches the name of the trap group (and hence, the value of eventCommunity). If nothing is configured, traps are sent to each group that has the rmon-alarm category configured.

The event community is not the same as an SNMP community.

Options ***community-name***—Name of the trap group that is used when generating a trap if the event is configured to send traps.

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

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Configuring RMON Alarms and Events on page 262
- Monitoring RMON MIB Tables on page 271
- Understanding RMON on page 217
- *Junos OS Network Management Configuration Guide*

community-name

Syntax community-name *community-name*;

Hierarchy Level [edit snmp v3 snmp-community *community-index*]

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

Description The community name defines an SNMP community. The SNMP community authorizes SNMPv1 or SNMPv2 clients. The access privileges associated with the configured security name define which MIB objects are available and the operations (notify, read, or write) allowed on those objects.

Options ***community-name***—Community string for an SNMPv1 or SNMPv2c community. If unconfigured, it is the same as the community index. If the name includes spaces, enclose it in quotation marks (" ").

NOTE: Community names must be unique. You cannot configure the same community name at the **[edit snmp community]** and **[edit snmp v3 snmp-community *community-index*]** hierarchy levels.

The community name at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level is encrypted and not displayed in the command-line interface (CLI).

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

Related Documentation
- *Configuring the SNMPv3 Community*

 Copyright © 2018, Juniper Networks, Inc.

contact

Syntax contact *contact*;

Hierarchy Level [edit snmp]

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

Description Define the value of the MIB II **sysContact** object, which is the contact person for the managed system.

Options ***contact***—Name of the contact person. If the name includes spaces, enclose it in quotation marks (" ").

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

Related Documentation
- *Configuring the System Contact on a Device Running Junos OS*

description

Syntax description *description*;

Hierarchy Level [edit snmp]

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 Define the value of the MIB II **sysDescription** object, which is the description of the system being managed.

Options ***description***—System description. If the name includes spaces, enclose it in quotation marks (" ").

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

Related Documentation
- *Configuring the System Description on a Device Running Junos OS*

description (RMON)

Syntax description *description*;

Hierarchy Level [edit snmp rmon alarm *index*],
[edit snmp rmon event *index*]

Release Information 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 Text description of alarm or event.

Options ***description***—Text description of an alarm or event entry. If the description includes spaces, enclose it in quotation marks (" ").

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

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Configuring RMON Alarms and Events on page 262
- Monitoring RMON MIB Tables on page 271
- Understanding RMON on page 217
- *Junos OS Network Management Configuration Guide*

 Copyright © 2018, Juniper Networks, Inc.

destination-port (SNMP)

Syntax destination-port *port-number*;

Hierarchy Level [edit snmp trap-group]

Release Information 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 Assign a trap port number other than the default.

Default If you omit this statement, the default port is 162.

Options ***port-number***—SNMP trap port number.

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

Related Documentation

- Configuring SNMP Trap Groups on page 258

engine-id

Syntax

```
engine-id {
   (local engine-id-suffix | use-default-ip-address | use-mac-address);
}
```

Hierarchy Level [edit snmp]

Release Information

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

Define a unique identifier for an SNMPv3 engine by configuring the suffix of the engine ID. The engine ID is used for identification only and not for addressing. There are two parts of an engine ID: the prefix and the suffix. The prefix is formatted according to the specifications defined in RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks* and cannot be configured. The suffix is configured here.

NOTE: SNMPv3 authentication and encryption keys are generated based on the associated user passwords and the engine ID. If you configure or change the engine ID, you must commit the user passwords and new engine ID before you configure SNMPv3 users, or the authentication will fail.

By default, the engine ID suffix is configured with the MAC address of the management interface (the use-mac-address option) on the QFX Series and OCX Series. You can override this configuration by using the local *engine-id-suffix* or use-default-ip-address option.

Default use-mac-address

Options

local *engine-id-suffix*—The engine ID suffix is set based on the data entered.

use-default-ip-address—The engine ID suffix is generated from the default IP address.

use-mac-address—The engine ID suffix is generated from the MAC address of the management interface on the switch.

Required Privilege Level

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

Related Documentation

- SNMPv3 Overview on page 215
- Configuring SNMP on page 254
- Minimum SNMPv3 Configuration on a Device Running Junos OS on page 216

Copyright © 2018, Juniper Networks, Inc.

event

Syntax

```
event index {
   community community-name;
   description description;
   type (RMON Notification) type;
}
```

Hierarchy Level

[edit snmp rmon]

Release Information

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 RMON event entries.

Options

index—Identifier for a specific event entry.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Monitoring RMON MIB Tables on page 271
- Understanding RMON on page 217
- *Junos OS Network Management Configuration Guide*

falling-event-index (RMON)

Syntax falling-event-index *index*;

Hierarchy Level [edit snmp rmon alarm *index*]

Release Information 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 Set the index number of the event entry that is used when a falling threshold is crossed. You specify the falling-event index when you configure an SNMP RMON alarm. If this value is zero, no event is triggered.

Options ***index***—Index of the event entry that is used when a falling threshold is crossed.

Range: 0 through 65,535

Default: 0

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

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Configuring RMON Alarms and Events on page 262
- Monitoring RMON MIB Tables on page 271
- Understanding RMON on page 217
- *Junos OS Network Management Configuration Guide*

 Copyright © 2018, Juniper Networks, Inc.

falling-threshold (Health Monitor)

Syntax falling-threshold *percentage*;

Hierarchy Level [edit snmp health-monitor]

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

Description Set the lower threshold for the monitored object when you configure a health monitor alarm. By setting a rising and a falling threshold for a monitored variable, you can be alerted whenever the value of the variable falls outside the allowable operational range.

Options ***percentage***—Lower threshold for the alarm entry.

Range: 1 through 100

Default: 70 percent of the maximum possible value

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

Related Documentation

- rising-threshold on page 342
- Configuring Health Monitoring on page 265

falling-threshold (RMON)

Syntax falling-threshold *integer*;

Hierarchy Level [edit snmp rmon alarm *index*]

Release Information 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 Set the lower threshold for the sampled variable (monitored object) when you configure an SNMP RMON alarm. By setting a rising and a falling threshold for a variable, you can be alerted whenever the value of the variable falls outside the allowable operational range.

Options ***integer***—Lower threshold for the alarm entry.

Range: –2,147,483,648 through 2,147,483,647

Default: 20 percent less than the **rising-threshold** value

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

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Configuring RMON Alarms and Events on page 262
- Monitoring RMON MIB Tables on page 271
- Understanding RMON on page 217
- *Junos OS Network Management Configuration Guide*

 Copyright © 2018, Juniper Networks, Inc.

falling-threshold-interval

Syntax falling-threshold-interval *seconds*;

Hierarchy Level [edit snmp rmon alarm *index*]

Release Information 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 Set the interval between samples after the rising threshold is exceeded and the value of the sample starts to drop. If the value of the sample drops and exceeds the falling threshold, the regular sampling interval is used.

Options ***interval***—Time between samples, in seconds.

Range: 1 through 2,147,483,647 seconds

Default: 60 seconds

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

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Configuring RMON Alarms and Events on page 262
- Monitoring RMON MIB Tables on page 271
- Understanding RMON on page 217
- *Junos OS Network Management Configuration Guide*

filter-duplicates

Syntax filter-duplicates;

Hierarchy Level [edit snmp]

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

Description Filter duplicate **Get**, **GetNext**, or **GetBulk** SNMP requests.

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

Related Documentation
- *Understanding the Implementation of SNMP on the QFabric System*
- Example: Configuring SNMP on page 279

filter-interfaces

Syntax

```
filter-interfaces {
   all-internal-interfaces;
   interfaces interface
}
```

Hierarchy Level [edit snmp]

Release Information 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 Filter out information related to specific interfaces from the output of SNMP **Get** and **GetNext** requests performed on interface-related MIBs.

Options

all-internal-interfaces—Filter out information from SNMP **Get** and **GetNext** requests for all internal interfaces.

interfaces—Filter out information from SNMP **Get** and **GetNext** requests for the specified interface.

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

Related Documentation
- *Filtering Interface Information Out of SNMP Get and GetNext Output*

 Copyright © 2018, Juniper Networks, Inc.

group (Defining Access Privileges for an SNMPv3 Group)

Syntax

group *group-name*;

Hierarchy Level

[edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c)
security-name *security-name*]

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

Define access privileges granted to a group.

Options

group-name—Identifies a collection of SNMP security names that belong to the same access policy SNMP.

Required Privilege Level

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

Related Documentation

- *Configuring the Group*

group (Configuring Group Name)

Syntax

```
group group-name {
  (default-context-prefix | context-prefix context-prefiix){
    security-model (any | usm | v1 | v2c) {
      security-level (authentication | none | privacy) {
        notify-view view-name;
        read-view view-name;
        write-view view-name;
      }
    }
  }
}
```

Hierarchy Level

[edit snmp v3 vacm access]

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

Assign the security name to a group, and specify the SNMPv3 context applicable to the group. The **default-context-prefix** statement, when included, adds all the contexts configured on the device to the group, whereas the **context-prefix** ***context-prefix*** statement enables you to specify a context and to add that particular context to the group.

(Not applicable to the QFX Series and OCX Series.) When the context prefix is specified as default (for example, **context-prefix default**), the context associated with the master routing instance is added to the group. To specify a routing instance that is part of a logical system, specify it as **logical system/routing instance**. For example, to specify routing instance ri1 in logical system ls1, include **context-prefix ls1/ri1**.

The remaining statements under this hierarchy are explained separately.

Options

group-name—SNMPv3 group name created for the SNMPv3 group.

Required Privilege Level

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

Related Documentation

- *Configuring the Group*

Copyright © 2018, Juniper Networks, Inc.

health-monitor

Syntax

```
health-monitor {
   falling-threshold percentage;
   interval seconds;
   rising-threshold percentage;
}
```

Hierarchy Level [edit snmp]

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

Description Configure health monitoring.

The remaining statements are explained separately. See CLI Explorer.

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

Related Documentation

- Configuring Health Monitoring on page 265
- Understanding Health Monitoring on page 221

history

Syntax

```
history history-index {
    bucket-size number;
    interface interface-name;
    interval seconds;
    owner owner-name;
}
```

Hierarchy Level

[edit snmp rmon]

Release Information

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 RMON history group entries. This RMON feature can be used with the Simple Network Management Protocol (SNMP) agent on the network to monitor all the traffic flowing among devices on all connected LAN segments. The RMON history feature collects statistics in accordance with user-configurable parameters.

The history group controls the periodic statistical sampling of data from various types of networks. This group contains configuration entries that specify an interface, polling period, and other parameters. If you use the **history** statement, you must also configure the interface ***interface-name*** statement.

Options

history-index—Provide a number for this history entry.

Range: 1 through 655535

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

snmp—To view this statement in the configuration.
snmp–control—To add this statement to the configuration.

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Monitoring RMON MIB Tables on page 271
- Understanding RMON on page 217
- *Junos OS Network Management Configuration Guide*

Copyright © 2018, Juniper Networks, Inc.

interface (SNMP)

Syntax interface [*interface-names*];

Hierarchy Level [edit snmp]

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 interfaces on which SNMP requests can be accepted.

Default If you omit this statement, SNMP requests entering the router or switch through any interface are accepted.

Options ***interface-names***—Names of one or more logical interfaces.

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

Related Documentation

- Configuring the Interfaces on Which SNMP Requests Can Be Accepted on page 260

interface (RMON)

Syntax interface *interface-name*;

Hierarchy Level [edit snmp rmon history *history-index*]

Release Information 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 the interface to be monitored in the specified RMON history entry.

Only one interface can be specified for a particular RMON history index. There is a one-to-one relationship between the interface and the history index. The interface must be specified in order for the RMON history to be created.

Options *interface-name*—Specify the interface to be monitored within the specified entry of the RMON history of Ethernet statistics.

Required Privilege Level snmp—To view this statement in the configuration.
snmp–control—To add this statement to the configuration.

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Configuring RMON Alarms and Events on page 262
- Monitoring RMON MIB Tables on page 271
- Understanding RMON on page 217
- *Junos OS Network Management Configuration Guide*

 Copyright © 2018, Juniper Networks, Inc.

interval (Health Monitor)

Syntax interval *seconds*;

Hierarchy Level [edit snmp health-monitor]

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

Description Configure the interval between sampling of the object being monitored by the health monitor.

Options ***seconds***—Time between samples, in seconds.

Range: **1** through **2147483647** seconds

Default: **300** seconds

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

Related Documentation

- Configuring Health Monitoring on page 265

interval (RMON)

Syntax interval *seconds*;

Hierarchy Level [edit snmp rmon alarm *index*],
[edit snmp rmon history *index*]

Release Information 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 interval over which data is to be sampled for the specified alarm or interface.

Default **60 sec** for alarm sampling.

1800 sec for history sampling.

Options ***seconds***—Interval at which data is to be sampled for the specified alarm or interface.

Required Privilege Level snmp—To view this statement in the configuration.
snmp–control—To add this statement to the configuration.

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Configuring RMON Alarms and Events on page 262
- Monitoring RMON MIB Tables on page 271
- Understanding RMON on page 217
- *Junos OS Network Management Configuration Guide*

 Copyright © 2018, Juniper Networks, Inc.

local-engine

Syntax

```
local-engine {
  user username {
    authentication-md5 {
      (authentication-key authentication-key | authentication-password
        authentication-password);
    }
    authentication-none;
    authentication-sha {
      (authentication-key authentication-key | authentication-password
        authentication-password);
    }
    privacy-aes128 {
      (privacy-key privacy-key | privacy-password privacy-password);
    }
    privacy-des {
      (privacy-key privacy-key | privacy-password privacy-password);
    }
    privacy-3des {
      (privacy-key privacy-key | privacy-password privacy-password);
    }
    privacy-none {
    }
  }
}
```

Hierarchy Level

[edit snmp v3 usm]

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 local engine information for the user-based security model (USM).

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Creating SNMPv3 Users on page 266

location

Syntax location *location*;

Hierarchy Level [edit snmp]

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

Description Define the value of the MIB II **sysLocation** object, which is the physical location of the managed system.

Options ***location***—Location of the local system. You must enclose the name within quotation marks (" ").

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

Related Documentation
- *Configuring the System Location for a Device Running Junos OS*

message-processing-model

Syntax message-processing-model (v1 | v2c | v3);

Hierarchy Level [edit snmp v3 target-parameters *target-parameter-name* parameters]

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 message processing model to be used when generating SNMP notifications.

Options **v1**—SNMPv1 message process model.

v2c—SNMPv2c message process model.

v3—SNMPv3 message process model.

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

Related Documentation
- *Configuring the Message Processing Model*

 Copyright © 2018, Juniper Networks, Inc.

name

Syntax name *name*;

Hierarchy Level [edit snmp]

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

Description Set the system name from the command-line interface.

Options ***name***—System name override.

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

Related Documentation
- *Configuring a Different System Name*

nonvolatile

Syntax

```
nonvolatile {
    commit-delay seconds;
}
```

Hierarchy Level [edit snmp]

Release Information 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 options for SNMP **Set** requests.

The remaining statement is explained separately. See CLI Explorer.

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

Related Documentation
- *Configuring the Commit Delay Timer*
- *commit-delay*

notify

Syntax

```
notify name {
   tag tag-name;
   type (trap | inform);
}
```

Hierarchy Level

[edit snmp v3]

Release Information

Statement introduced before Junos OS Release 7.4.
type inform option added in 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

Select management targets for SNMPv3 notifications as well as the type of notifications. Notifications can be either traps or informs.

Options

name—Name assigned to the notification.

tag-name—Notifications are sent to all targets configured with this tag.

type—Notification type is **trap** or **inform**. Traps are unconfirmed notifications. Informs are confirmed notifications.

Required Privilege Level

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

Related Documentation

- *Configuring the Inform Notification Type and Target Address*
- *Configuring the SNMPv3 Trap Notification*

Copyright © 2018, Juniper Networks, Inc.

notify-filter (Applying to the Management Target)

Syntax notify-filter *profile-name*;

Hierarchy Level [edit snmp v3 target-parameters *target-parameters-name*]

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 the notify filter to be used by a specific set of target parameters.

Options ***profile-name***—Name of the notify filter to apply to notifications.

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

Related Documentation
- *Applying the Trap Notification Filter*

notify-filter (Configuring the Profile Name)

Syntax

```
notify-filter profile-name {
   oid oid (include | exclude);
}
```

Hierarchy Level

[edit snmp v3]

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 group of MIB objects for which you define access. The notify filter limits the type of traps or informs sent to the network management system.

Options

profile-name—Name assigned to the notify filter.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring the Trap Notification Filter*
- *oid*

Copyright © 2018, Juniper Networks, Inc.

notify-view

Syntax notify-view *view-name*;

Hierarchy Level [edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]

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 Associate the notify view with a community (for SNMPv1 or SNMPv2c clients) or a group name (for SNMPv3 clients).

Options ***view-name***—Name of the view to which the SNMP user group has access.

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

Related Documentation
- Configuring MIB Views on page 261
- *Configuring the Notify View*

oid

Syntax oid *object-identifier* (exclude| include);

Hierarchy Level [edit snmp view *view-name*]

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

Description Specify an object identifier (OID) used to represent a subtree of MIB objects.

Options **exclude**—Exclude the subtree of MIB objects represented by the specified OID.

include—Include the subtree of MIB objects represented by the specified OID.

object-identifier—OID used to represent a subtree of MIB objects. All MIB objects represented by this statement have the specified OID as a prefix. You can specify the OID using either a sequence of dotted integers or a subtree name.

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

 Copyright © 2018, Juniper Networks, Inc.

oid (SNMPv3)

Syntax oid *oid* (include | exclude);

Hierarchy Level [edit snmp v3 notify-filter *profile-name*]

Release Information 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 an object identifier (OID) used to represent a subtree of MIB objects. This OID is a prefix that the represented MIB objects have in common.

Options

exclude—Exclude the subtree of MIB objects represented by the specified OID.

include—Include the subtree of MIB objects represented by the specified OID.

oid—Object identifier used to represent a subtree of MIB objects. All MIB objects represented by this statement have the specified OID as a prefix. You can specify the OID using either a sequence of dotted integers or a subtree name.

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

Related Documentation

- SNMPv3 Overview on page 215
- Minimum SNMPv3 Configuration on a Device Running Junos OS on page 216
- Configuring SNMP on page 254
- *Configuring the SNMPv3 Trap Notification*

owner

Syntax owner *owner-name*;

Hierarchy Level [edit snmp rmon history *index*]

Release Information 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 the user or group responsible for this RMON history configuration.

Options ***owner-name***—User or group responsible for this configuration.

Range: 0 through 32 alphanumeric characters

Required Privilege Level snmp—To view this statement in the configuration.
snmp–control—To add this statement to the configuration.

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Configuring RMON Alarms and Events on page 262
- Monitoring RMON MIB Tables on page 271
- Understanding RMON on page 217
- *Junos OS Network Management Configuration Guide*

 Copyright © 2018, Juniper Networks, Inc.

parameters

Syntax

```
parameters {
  message-processing-model (v1 | v2c | v3);
  security-level (none | authentication | privacy);
  security-model (usm | v1 | v2c);
  security-name security-name;
}
```

Hierarchy Level

[edit snmp v3 target-parameters *target-parameters-name*]

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 a set of target parameters for message processing and security.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Defining and Configuring the Trap Target Parameters*

port

Syntax port *port-number*;

Hierarchy Level [edit snmp v3 target-address *target-address-name*]

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 a UDP port number for an SNMP target.

Default If you omit this statement, the default port is 162.

Options ***port-number***—Port number for the SNMP target.

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

Related Documentation

- *Configuring the Port*

Copyright © 2018, Juniper Networks, Inc.

privacy-3des

Syntax

```
privacy-3des {
   (privacy-key privacy-key | privacy-password privacy-password);
}
```

Hierarchy Level

[edit snmp v3 usm local-engine user *username*],
[edit snmp v3 usm remote-engine *engine-id* 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.

Description

Configure the triple Data Encryption Standard (3DES) as the privacy type for the SNMPv3 user.

For privacy encryption, you can either enter a password in clear text, which is immediately encrypted, or, if you already have the encrypted version (known as a *key*), enter the key directly.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring the SNMPv3 Encryption Type*

privacy-aes128

Syntax

```
privacy-aes128 {
   (privacy-key privacy-key | privacy-password privacy-password);
}
```

Hierarchy Level

[edit snmp v3 usm local-engine user *username*],
[edit snmp v3 usm remote-engine *engine-id* 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.

Description

Configure the Advanced Encryption Standard encryption algorithm (CFB128-AES-128 Privacy Protocol) for the SNMPv3 user.

For privacy encryption, you can either enter a password in clear text, which is immediately encrypted, or, if you already have the encrypted version (known as a *key*), enter the key directly.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring the SNMPv3 Encryption Type*

Copyright © 2018, Juniper Networks, Inc.

privacy-des

Syntax

```
privacy-des {
   (privacy-key privacy-key | privacy-password privacy-password);
}
```

Hierarchy Level

[edit snmp v3 usm local-engine user *username*],
[edit snmp v3 usm remote-engine *engine-id* 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.

Description

Configure the Data Encryption Standard (DES) as the privacy type for the SNMPv3 user.

For privacy encryption, you can either enter a password in clear text, which is immediately encrypted, or, if you already have the encrypted version (known as a *key*), enter the key directly.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring the SNMPv3 Encryption Type*

privacy-none

Syntax

```
privacy-none;
```

Hierarchy Level

[edit snmp v3 usm local-engine user *username*],
[edit snmp v3 usm remote-engine *engine-id* 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.

Description

Configure that no encryption be used for the SNMPv3 user.

Required Privilege Level

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

Related Documentation

- *Configuring the SNMPv3 Encryption Type*

privacy-password

Syntax

privacy-password *privacy-password*;

Hierarchy Level

[edit snmp v3 usm local-engine user *username* privacy-3des],
[edit snmp v3 usm local-engine user *username* privacy-aes128],
[edit snmp v3 usm local-engine user *username* privacy-des],
[edit snmp v3 usm remote-engine *engine-id* user *username* privacy-3des],
[edit snmp v3 usm remote-engine *engine-id* user *username* privacy-aes128],
[edit snmp v3 usm remote-engine *engine-id* user *username* privacy-des]

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 a privacy password for the SNMPv3 user.

Options

privacy-password—Password that a user enters. The password is then converted into a key that is used for encryption.

SNMPv3 has special requirements when you create plain-text passwords on a router or switch:

- The password must be at least eight characters long.
- The password can include alphabetic, numeric, and special characters, but it cannot include control characters.

Required Privilege Level

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

Related Documentation

- *Configuring the SNMPv3 Encryption Type*

Copyright © 2018, Juniper Networks, Inc.

read-view

Syntax read-view *view-name*;

Hierarchy Level [edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]

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 Associate the read-only view with a community (for SNMPv1 or SNMPv2c clients) or a group name (for SNMPv3 clients).

Options ***view-name***—The name of the view to which the SNMP user group has access.

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

Related Documentation

- *Configuring the Read View*
- Configuring MIB Views on page 261

remote-engine

Syntax

```
remote-engine engine-id {
  user username {
    authentication-md5 {
      (authentication-key authentication-key | authentication-password
        authentication-password);
    }
    authentication-none;
    authentication-sha {
      (authentication-key authentication-key | authentication-password
        authentication-password);
    }
    privacy-aes128 (privacy-key privacy-key | privacy-password privacy-password);
    }
    privacy-des {
      (privacy-key privacy-key | privacy-password privacy-password);
    }
    privacy-3des {
      (privacy-key privacy-key | privacy-password privacy-password);
    }
    privacy-none {
    }
  }
}
```

Hierarchy Level

[edit snmp v3 usm]

Release Information

Statement introduced in 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 remote engine information for the user-based security model (USM). To send inform messages to an SNMPv3 user on a remote device, you must configure the engine identifier for the SNMP agent on the remote device where the user resides.

Options

engine-id—Specify engine identifier in hexadecimal format. Used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring the Remote Engine and Remote User*

Copyright © 2018, Juniper Networks, Inc.

request-type

Syntax request-type (get-next-request | get-request | walk-request);

Hierarchy Level [edit snmp rmon alarm *index*]

Release Information 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 Extend monitoring to a specific SNMP object instance (get-request), to all object instances belonging to a MIB branch (walk-request), or to the next object instance after the instance specified in the configuration (get-next-request).

Default **walk-request**

Options **get-next-request**—Perform an SNMP get next request.

get-request—Perform an SNMP get request.

walk-request—Perform an SNMP walk request.

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

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Configuring RMON Alarms and Events on page 262
- Monitoring RMON MIB Tables on page 271
- Understanding RMON on page 217
- *Junos OS Network Management Configuration Guide*

retry-count

Syntax retry-count *number*;

Hierarchy Level [edit snmp v3 target-address *target-address-name*]

Release Information Statement introduced in Junos OS Release 7.4.

Description Configure the retry count for SNMP informs.

Options ***number***—Maximum number of times the inform is transmitted if no acknowledgment is received. If no acknowledgment is received after the inform is transmitted the maximum number of times, the inform message is discarded.

Default: 3 times

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

Related Documentation

- Configuring SNMP Informs on page 270
- *timeout*

 Copyright © 2018, Juniper Networks, Inc.

rising-event-index

Syntax rising-event-index *index*;

Hierarchy Level [edit snmp rmon alarm *index*]

Release Information 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 Set the index of the event entry that is used when a rising alarm threshold is exceeded. The rising-event index is specified when you configure an SNMP RMON alarm. If this value is zero, no event is triggered.

Options ***index***—Index of the event entry that is used when a rising threshold is exceeded.

Range: 0 through 65,535

Default: 0

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

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Configuring RMON Alarms and Events on page 262
- Monitoring RMON MIB Tables on page 271
- Understanding RMON on page 217
- *Junos OS Network Management Configuration Guide*

rising-threshold (Health Monitor)

Syntax rising-threshold *percentage*;

Hierarchy Level [edit snmp health-monitor]

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

Description Set the upper threshold for the monitored object when you configure a health monitor alarm. By setting a rising and a falling threshold for a monitored object, you can be alerted whenever the value of the variable falls outside the allowable operational range.

Options *percentage*—Upper threshold for the alarm entry.

Range: 1 through 100

Default: 80 percent of the maximum possible value

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

Related Documentation

- Configuring Health Monitoring on page 265
- **falling-threshold on page 309**

 Copyright © 2018, Juniper Networks, Inc.

rising-threshold (RMON)

Syntax rising-threshold *integer*;

Hierarchy Level [edit snmp rmon alarm *index*]

Release Information 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 Set the upper threshold for the sampled variable (monitored object) when you configure an SNMP RMON alarm. By setting a rising and a falling threshold for a variable, you can be alerted whenever the value of the variable falls outside the allowable operational range.

Options *integer*—Upper threshold for the alarm entry.

Range: –2,147,483,648 through 2,147,483,647

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

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Configuring RMON Alarms and Events on page 262
- Monitoring RMON MIB Tables on page 271
- Understanding RMON on page 217
- *Junos OS Network Management Configuration Guide*

rmon

Syntax

```
rmon {
  alarm index {
    description description;
    falling-event-index index;
    falling-threshold integer;
    falling-threshold-interval seconds;
    interval seconds;
    request-type;
    rising-event-index index;
    rising-threshold integer;
    sample-type (absolute-value | delta-value);
    startup-alarm (falling-alarm | rising-alarm | rising-or-falling alarm);
    syslog-subtag syslog-subtag;
    variable oid-variable;
  }
  event index {
    community community-name;
    description description;
    type (RMON Notification) type;
  }
  history history-index {
    bucket-size number;
    interface interface-name;
    interval seconds;
    owner owner-name;
  }
}
```

Hierarchy Level [edit snmp]

Release Information 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 Provide comprehensive network fault diagnosis, planning, and performance tuning information. RMON delivers this information in nine groups of monitoring elements, each providing specific sets of data to meet common network monitoring requirements. Each group is optional, so that vendors do not need to support all the groups within the MIB.

Junos OS supports the RMON statistics, history, alarm, and event groups.

The remaining statements are explained separately. See CLI Explorer.

Default Disabled.

Required Privilege Level snmp—To view this statement in the configuration.
snmp–control—To add this statement to the configuration.

 Copyright © 2018, Juniper Networks, Inc.

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Monitoring RMON MIB Tables on page 271
- Understanding RMON on page 217
- *Junos OS Network Management Configuration Guide*

sample-type

Syntax

sample-type (absolute-value | delta-value);

Hierarchy Level

[edit snmp rmon alarm *index*]

Release Information

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 method of sampling the selected variable (monitored object). When you configure an SNMP RMON alarm, you can specify the sample type.

Options

absolute-value—Actual value of the selected variable is used when comparing against the thresholds.

delta-value—Difference between samples of the selected variable is used when comparing against the thresholds.

Required Privilege Level

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

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Configuring RMON Alarms and Events on page 262
- Monitoring RMON MIB Tables on page 271
- Understanding RMON on page 217
- *Junos OS Network Management Configuration Guide*

security-level (Defining Access Privileges)

Syntax

```
security-level (authentication | none | privacy) {
  notify-view view-name;
  read-view view-name;
  write-view view-name;
}
```

Hierarchy Level

[edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*) security-model (any | usm | v1 | v2c)]

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

Define the security level used for access privileges.

Default

none

Options

authentication—Provide authentication but no encryption.

none—No authentication and no encryption.

privacy—Provide authentication and encryption.

Required Privilege Level

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

Related Documentation

- *Configuring the Security Level*

Copyright © 2018, Juniper Networks, Inc.

security-level (Generating SNMP Notifications)

Syntax security-level (authentication | none | privacy);

Hierarchy Level [edit snmp v3 target-parameters *target-parameters-name* parameters]

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 security level to use when generating SNMP notifications.

Default none

Options **authentication**—Provide authentication but no encryption.

none—No authentication and no encryption.

privacy—Provide authentication and encryption.

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

Related Documentation

- *Configuring the Security Level*

security-model (Access Privileges)

Syntax security-model (usm | v1 | v2c);

Hierarchy Level [edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*)]

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 security model for an SNMPv3 group. The security model is used to determine access privileges for the group.

Options **usm**—SNMPv3 security model.

v1—SNMPv1 security model.

v2c—SNMPv2c security model.

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

Related Documentation
- *Configuring the Security Model*

 Copyright © 2018, Juniper Networks, Inc.

security-model (Group)

Syntax

```
security-model (usm | v1 | v2c) {
  security-name security-name {
    group group-name;
  }
}
```

Hierarchy Level

[edit snmp v3 vacm security-to-group]

Release Information

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

Description

Define a security model for a group.

Options

usm—SNMPv3 security model.

v1—SNMPv1 security model.

v2c—SNMPv2c security model.

Required Privilege Level

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

Related Documentation

- *Configuring the Security Model*

security-model (SNMP Notifications)

Syntax security-model (usm | v1 | v2c);

Hierarchy Level [edit snmp v3 target-parameters *target-parameters-name* parameters]

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 security model for an SNMPv3 group. The security model is used for SNMP notifications.

Options

usm—SNMPv3 security model.

v1—SNMPv1 security model.

v2c—SNMPv2c security model.

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

Related Documentation

- *Configuring the Security Model*

Copyright © 2018, Juniper Networks, Inc.

security-name (Community String)

Syntax security-name *security-name*;

Hierarchy Level [edit snmp v3 snmp-community *community-index*]

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 Associate a community string with the security name of a user. The community string, which is used for SNMPv1 and SNMPv2c clients in an SNMPv3 system, is configured at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level.

Options ***security-name***—Name that is used for messaging security and user access control.

NOTE: The security name must match the configured security name at the **[edit snmp v3 target-parameters *target-parameters-name* parameters]** hierarchy level when you configure traps or informs.

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

Related Documentation

- *Configuring the Security Names*

security-name (Security Group)

Syntax

```
security-name security-name {
  group group-name;
}
```

Hierarchy Level

[edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c)]

Release Information

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

Description

Associate a group or a community string with a configured security group.

Options

security-name—Username configured at the **[edit snmp v3 usm local-engine user *username*]** hierarchy level. For SNMPv1 and SNMPv2c, the security name is the community string configured at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level.

Required Privilege Level

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

Related Documentation

- *Assigning Security Names to Groups*

Copyright © 2018, Juniper Networks, Inc.

security-name (SNMP Notifications)

Syntax security-name *security-name*;

Hierarchy Level [edit snmp v3 target-parameters *target-parameters-name* parameters]

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 security name used when generating SNMP notifications.

Options ***security-name***—If the SNMPv3 USM security model is used, identify the user when generating the SNMP notification. If the v1 or v2c security models are used, identify the SNMP community used when generating the notification.

NOTE: The access privileges for the group associated with this security name must allow this notification to be sent.

If you are using the v1 or v2 security models, the security name at the **[edit snmp v3 vacm security-to-group]** hierarchy level must match the security name at the **[edit snmp v3 snmp-community *community-index*]** hierarchy level.

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

Related Documentation

- *Configuring the Security Name*

security-to-group

Syntax

```
security-to-group {
  security-model (usm | v1 | v2c) {
    group group-name;
    security-name security-name;
  }
}
```

Hierarchy Level

[edit snmp v3 vacm]

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 group to which a specific SNMPv3 security name belongs. The security name is used for messaging security.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Assigning Security Model and Security Name to a Group*

Copyright © 2018, Juniper Networks, Inc.

snmp

Syntax

```
snmp {
  client-list client-list-name {
    ip-addresses;
  }
  community community-name {
    authorization authorization;
    client-list-name client-list-name;
    clients {
      address restrict;
    }
    logical-system logical-system-name {
      routing-instance routing-instance-name {
        clients {
        addresses;
        }
      }
    }
    routing-instance routing-instance-name {
      clients {
      addresses;
      }
    }
    view view-name;
  }
  contact contact;
  description description;
  filter-duplicates;
  filter-interfaces;
  health-monitor {
    falling-threshold integer;
    interval seconds;
    rising-threshold integer;
  }
  interface [ interface-names ];
  location location;
  name name;
  nonvolatile {
    commit-delay seconds;
  }
  rmon {
    alarm index {
      description description;
      falling-event-index index;
      falling-threshold integer;
      falling-threshold-interval seconds;
      interval seconds;
      request-type;
      rising-event-index index;
      rising-threshold integer;
      sample-type (absolute-value | delta-value);
      startup-alarm (falling-alarm | rising-alarm | rising-or-falling alarm);
      syslog-subtag syslog-subtag;
```

```
        variable oid-variable;
    }
    event index {
        community community-name;
        description description;
        type type;
    }
    history history-index {
        bucket-size number;
        interface interface-name;
        interval seconds;
        owner owner-name;
    }
}
traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable> <match
        regular-expression>;
    flag flag;
}
trap-group group-name {
    categories {
        category;
    }
    destination-port port-number;
    routing-instance routing-instance-name;
    targets {
        address;
    }
    version (all | v1 | v2);
}
trap-options {
    agent-address outgoing-interface;
    source-address address;
}
v3 {
    notify name {
        tag tag-name;
        type trap;
    }
    notify-filter profile-name {
        oid object-identifier (include | exclude);
    }
    snmp-community community-index {
        community-name community-name;
        security-name security-name;
        tag tag-name;
    }
    target-address target-address-name {
        address address;
        address-mask address-mask;
        logical-system logical-system;
        port port-number;
        retry-count number;
        routing-instance routing-instance-name;
        tag-list tag-list;
        target-parameters target-parameters-name;
```


Copyright © 2018, Juniper Networks, Inc.

```
    timeout seconds;
  }
  target-parameters target-parameters-name {
    notify-filter profile-name;
    parameters {
      message-processing-model (v1 | v2c | V3);
      security-level (authentication | none | privacy);
      security-model (usm | v1 | v2c);
      security-name security-name;
    }
  }
  usm {
    local-engine {
      user username {
        authentication-sha {
          authentication-password authentication-password;
        }
        authentication-md5 {
          authentication-password authentication-password;
        }
        authentication-none;
        privacy-aes128 {
          privacy-password privacy-password;
        }
        privacy-des {
          privacy-password privacy-password;
        }
        privacy-3des {
          privacy-password privacy-password;
        }
        privacy-none;
      }
    }
    remote-engine engine-id {
      user username {
        authentication-sha {
          authentication-password authentication-password;
        }
        authentication-md5 {
          authentication-password authentication-password;
        }
        authentication-none;
        privacy-aes128 {
          privacy-password privacy-password;
        }
        privacy-des {
          privacy-password privacy-password;
        }
        privacy-3des {
          privacy-password privacy-password;
        }
        privacy-none {
          privacy-password privacy-password;
        }
      }
    }
```

```
        }
        vacm {
          access {
            group group-name {
              (default-context-prefix | context-prefix context-prefix) {
                security-model (any | usm | v1 | v2c) {
                  security-level (authentication | none | privacy) {
                    notify-view view-name;
                    read-view view-name;
                    write-view view-name;
                  }
                }
              }
            }
          }
          security-to-group {
            security-model (usm | v1 | v2c) {
              security-name security-name {
                group group-name;
              }
            }
          }
        }
      }
      view view-name {
        oid object-identifier (include | exclude);
      }
    }
}
```

Hierarchy Level [edit]

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

Description Configure SNMP.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level snmp—To view this statement in the configuration.
snmp–control—To add this statement to the configuration.

Related Documentation

- Understanding the Implementation of SNMP on page 212
- Configuring SNMP on page 254

 Copyright © 2018, Juniper Networks, Inc.

snmp-community

Syntax

```
snmp-community community-index {
    community-name community-name;
    security-name security-name;
    tag tag-name;
}
```

Hierarchy Level

[edit snmp v3]

Release Information

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

Description

Configure the SNMP community.

Options

community-index—(Optional) String that identifies an SNMP community.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- *Configuring the SNMPv3 Community*

source-address (SNMP)

Syntax source-address *address*;

Hierarchy Level [edit snmp trap-options]

Release Information 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 Set the source address of every SNMP trap packet sent by this switch to a single address regardless of the outgoing interface. If the source address is not specified, the default is to use the address of the outgoing interface as the source address.

Options ***address***—Source address of SNMP traps. You can configure the source address of trap packets two ways: **lo0** or a valid IPv4 address configured on one of the interfaces. The value **lo0** indicates that the source address of all SNMP trap packets is set to the lowest loopback address configured at interface **lo0**.

Default: Disabled. (The source address is the address of the outgoing interface.)

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

Related Documentation

- *Configuring the Source Address for SNMP Traps*

 Copyright © 2018, Juniper Networks, Inc.

startup-alarm

Syntax startup-alarm (falling-alarm | rising-alarm | rising-or-falling-alarm);

Hierarchy Level [edit snmp rmon alarm *index*]

Release Information 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 Set an initial alarm that is sent after the configured SNMP RMON alarm becomes active.

Default **rising-or-falling-alarm**

Options

falling-alarm—Generated if the first sample after the alarm becomes active is equal to or greater than the falling threshold.

rising-alarm—Generated if the first sample after the alarm becomes active is equal to or greater than the rising threshold.

rising-or-falling-alarm—Generated if the first sample after the alarm entry becomes active is equal to or greater than either the rising threshold or the falling threshold.

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

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Configuring RMON Alarms and Events on page 262
- Monitoring RMON MIB Tables on page 271
- Understanding RMON on page 217
- *Junos OS Network Management Configuration Guide*

syslog-subtag

Syntax syslog-subtag *syslog-subtag*;

Hierarchy Level [edit snmp rmon alarm *index*]

Release Information 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 Add the **syslog-subtag** tag to the system log message. The tag should not exceed 80 uppercase characters.

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

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Monitoring RMON MIB Tables on page 271
- Understanding RMON on page 217
- *Junos OS Network Management Configuration Guide*

 Copyright © 2018, Juniper Networks, Inc.

tag (Configuring Notification Targets)

Syntax tag *tag-name*;

Hierarchy Level [edit snmp v3 notify *name*]

Release Information 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 a set of target addresses to receive SNMP traps or informs (for IPv4 packets only).

Options ***tag-name***—Define the target addresses to which an SNMP notification is sent. Target addresses containing the same tag in their tag list are sent the same notification. The ***tag-name*** is not included in the notification.

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

Related Documentation

- SNMPv3 Overview on page 215
- Minimum SNMPv3 Configuration on a Device Running Junos OS on page 216
- Configuring SNMP on page 254
- *Configuring the SNMPv3 Trap Notification*

tag-list

Syntax tag-list *tag-list*;

Hierarchy Level [edit snmp v3 target-address *target-address-name*]

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 an SNMP tag list used to select target addresses.

Options ***tag-list***—Define sets of target addresses (tags). To specify more than one tag, specify the tag names as a space-separated list enclosed within double quotes.

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

Related Documentation

- *Configuring the Trap Target Address*

 Copyright © 2018, Juniper Networks, Inc.

target-address

Syntax

```
target-address target-address-name {
    address address;
    address-mask address-mask;
    port port-number;
    retry-count number;
    tag-list tag-list;
    target-parameters target-parameters-name;
    timeout seconds;
}
```

Hierarchy Level

[edit snmp v3]

Release Information

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 address of an SNMP management application and the parameters to be used in sending notifications.

Options

target-address-name—String that identifies the target address.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Understanding the Implementation of SNMP on page 212
- SNMP MIBs Support on page 223
- SNMP Traps Support on page 236
- **snmp on page 355**
- Configuring SNMP on page 254
- Monitoring SNMP on page 272
- Example: Configuring SNMP on page 279

target-parameters

Syntax

At the **[edit snmp v3]** hierarchy level:

```
target-parameters target-parameters-name {
  profile-name;
  parameters {
    message-processing-model (v1 | v2c | V3);
    security-level (authentication | none | privacy);
    security-model (usm | v1 | v2c);
    security-name security-name;
  }
}
```

At the **[edit snmp v3 target-address *target-address-name*]** hierarchy level:

```
target-parameters target-parameters-name;
```

Hierarchy Level

[edit snmp v3]
[edit snmp v3 target-address *target-address-name*]

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 message processing and security parameters for sending notifications to a particular management target. The target parameters are configured at the **[edit snmp v3]** hierarchy level. The remaining statements at this level are explained separately.

Then apply the target parameters configured at the **[edit snmp v3 target-parameters *target-parameters-name*]** hierarchy level to the target address configuration at the **[edit snmp v3]** hierarchy level.

Required Privilege Level

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

Related Documentation

- *Defining and Configuring the Trap Target Parameters*
- *Applying Target Parameters*

Copyright © 2018, Juniper Networks, Inc.

targets

Syntax

```
targets {
  address;
}
```

Hierarchy Level

[edit snmp trap-group *group-name*]

Release Information

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

Description

Configure one or more systems to receive SNMP traps.

Options

address—IPv4 or IPv6 address of the system to receive traps. You must specify an address, not a hostname.

Required Privilege Level

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

Related Documentation

- Configuring SNMP Trap Groups on page 258

timeout

Syntax timeout *seconds*;

Hierarchy Level [edit snmp v3 target-address *target-address-name*]

Release Information 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 timeout period (in seconds) for SNMP informs.

Default **15** seconds

Options ***seconds***—Number of seconds to wait for an inform acknowledgment. If no acknowledgment is received within the timeout period, the inform is retransmitted.

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

Related Documentation

- Understanding the Implementation of SNMP on page 212
- Configuring SNMP Informs on page 270
- **retry-count on page 340**

 Copyright © 2018, Juniper Networks, Inc.

traceoptions (SNMP)

Syntax

```
traceoptions {
  file filename <files number> <match regular-expression> <size size> <world-readable |
    no-world-readable>;
  flag flag;
  no-remote-trace;
}
```

Hierarchy Level [edit snmp]

Release Information 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 Track the activities of SNMP agents on the switch and record the information in log files.

NOTE: The **traceoptions** statement is not supported on the QFabric system.

The output of the tracing operations is placed into log files in the **/var/log** directory. Each log file is named after the SNMP agent that generates it. The following logs are created in the **/var/log** directory when the **traceoptions** statement is used:

- chassisd
- craftd
- ilmid
- mib2d
- rmopd
- serviced
- snmpd

Options **file *filename***—By default, the name of the log file that records trace output is the name of the process being traced (for example, mib2d or snmpd). Use this option to specify another name.

files *number*—(Optional) Maximum number of trace files per SNMP subagent. When a trace file (for example, snmpd) reaches its maximum size, it is archived by being renamed to snmpd.0. The previous snmpd.1 is renamed to snmpd.2, and so on. The oldest archived file is deleted.

Range: 2 through 1000 files

Default: 10 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements:

- **all**—Log all SNMP events.
- **configuration**—Log reading of configuration at the **[edit snmp]** hierarchy level.
- **database**—Log events involving storage and retrieval in the events database.
- **events**—Log important events.
- **general**—Log general events.
- **interface-stats**—Log physical and logical interface statistics.
- **nonvolatile-sets**—Log nonvolatile SNMP set request handling.
- **pdu**—Log SNMP request and response packets.
- **policy**—Log policy processing.
- **protocol-timeouts**—Log SNMP response timeouts.
- **routing-socket**—Log routing socket calls.
- **server**—Log communication with processes that are generating events.
- **subagent**—Log subagent restarts.
- **timer-events**—Log internally generated events.
- **varbind-error**—Log variable binding errors.

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

size *size*—(Optional) Maximum size, in kilobytes (KB), of each trace file before it is closed and archived.

Range: 10 KB through 1 GB

Default: 1000 KB

world-readable | no-world-readable—(Optional) 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.

Required Privilege Level

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

Related Documentation

- Understanding Tracing and Logging Operations on page 6
- Tracing SNMP Activity on a Device Running Junos OS on page 274

Copyright © 2018, Juniper Networks, Inc.

trap-group

Syntax

```
trap-group group-name {
  categories {
    category;
  }
  destination-port port-number;
  targets {
    address;
  }
}
```

Hierarchy Level

[edit snmp]

Release Information

Statement introduced in Junos OS Release 11.1 for QFX Series switches.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Create a named group of hosts to receive the specified trap notifications. The name of the trap group is embedded in SNMP trap notification packets as one variable binding (varbind) known as the community name. At least one trap group must be configured for SNMP traps to be sent.

Options

group-name—Name of the trap group. If the name includes spaces, enclose it in quotation marks (" ").

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Configuring SNMP Trap Groups on page 258

trap-options

Syntax

```
trap-options {
  agent-address outgoing-interface;
  source-address address;
}
```

Hierarchy Level [edit snmp]

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

Description Using SNMP trap options, you can set the source address of every SNMP trap packet sent by the router or switch to a single address, regardless of the outgoing interface. In addition, you can set the agent address of each SNMPv1 trap. For more information about the contents of SNMPv1 traps, see RFC 1157.

The remaining statements are explained separately. See CLI Explorer.

Default Disabled

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

Related Documentation

- *Configuring SNMP Trap Options*

Copyright © 2018, Juniper Networks, Inc.

type (RMON Notification)

Syntax type *type*;

Hierarchy Level [edit snmp rmon event *index*]

Release Information 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 type of notification generated when a rising or falling threshold is crossed.

Default **log-and-trap**

Options *type*—Type of notification. It can be one of the following:

- **log**—Add an entry to the **logTable** object.
- **log-and-trap**—Send an SNMP trap and add a log entry.
- **none**—No notifications are sent.
- **snmptrap**—Send an SNMP trap.

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

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Configuring RMON Alarms and Events on page 262
- Monitoring RMON MIB Tables on page 271
- Understanding RMON on page 217
- *Junos OS Network Management Configuration Guide*

type

Syntax type (inform | trap);

Hierarchy Level [edit snmp v3 notify *name*]

Release Information Statement introduced before Junos OS Release 7.4.
inform option added in 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 type of SNMP notification.

Options **inform**—Defines the type of notification as an inform. SNMP informs are confirmed notifications.

trap—Defines the type of notification as a trap. SNMP traps are unconfirmed notifications.

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

Related Documentation

- Configuring SNMP Informs on page 270
- *Configuring the SNMPv3 Trap Notification*

 Copyright © 2018, Juniper Networks, Inc.

user

Syntax user *username*;

Hierarchy Level [edit snmp v3 usm local-engine],
[edit snmp v3 usm remote-engine *engine-id*]

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 user associated with an SNMPv3 group on a local or remote SNMP engine.

Options ***username***—SNMPv3 user-based security model (USM) username.

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

Related Documentation

- Creating SNMPv3 Users on page 266

usm

Syntax

```
usm {
  local-engine {
    user username {
      authentication-md5 {
        authentication-password authentication-password;
      }
      authentication-none;
      authentication-sha {
        authentication-password authentication-password;
      }
      privacy-aes128 {
        privacy-password privacy-password;
      }
      privacy-des {
        privacy-password privacy-password;
      }
      privacy-3des {
        privacy-password privacy-password;
      }
      privacy-none {
        privacy-password privacy-password;
      }
    }
    remote-engine engine-id {
      user username {
        authentication-md5 {
          authentication-password authentication-password;
        }
        authentication-none;
        authentication-sha {
          authentication-password authentication-password;
        }
        privacy-aes128 {
          privacy-password privacy-password;
        }
        privacy-des {
          privacy-password privacy-password;
        }
        privacy-3des {
          privacy-password privacy-password;
        }
        privacy-none {
          privacy-password privacy-password;
        }
      }
    }
  }
}
```

Hierarchy Level [edit snmp v3]

Copyright © 2018, Juniper Networks, Inc.

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 user-based security model (USM) information.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Creating SNMPv3 Users on page 266
- *Configuring the Remote Engine and Remote User*

v3

Syntax

```
v3 {
  notify name {
    tag tag-name;
    type trap;
  }
  notify-filter profile-name {
    oid object-identifier (include | exclude);
  }
  snmp-community community-index {
    community-name community-name;
    security-name security-name;
    tag tag-name;
  }
  target-address target-address-name {
    address address;
    address-mask address-mask;
    port port-number;
    retry-count number;
    tag-list tag-list;
    target-parameters target-parameters-name;
    timeout seconds;
  }
  target-parameters target-parameters-name {
    notify-filter profile-name;
    parameters {
      message-processing-model (v1 | v2c | V3);
      security-level (authentication | none | privacy);
      security-model (usm | v1 | v2c);
      security-name security-name;
    }
  }
  usm {
    local-engine {
      user username {
        authentication-md5 {
          authentication-password authentication-password;
        }
        authentication-sha {
          authentication-password authentication-password;
        }
        authentication-none;
        privacy-aes128 {
          privacy-password privacy-password;
        }
        privacy-des {
          privacy-password privacy-password;
        }
        privacy-3des {
          privacy-password privacy-password;
        }
        privacy-none;
      }
```


Copyright © 2018, Juniper Networks, Inc.

```
        }
        remote-engine engine-id {
          user username {
            authentication-md5 {
              authentication-password authentication-password;
            }
            authentication-sha {
              authentication-password authentication-password;
            }
            authentication-none;
            privacy-aes128 {
              privacy-password privacy-password;
            }
            privacy-des {
              privacy-password privacy-password;
            }
            privacy-3des {
              privacy-password privacy-password;
            }
            privacy-none {
              privacy-password privacy-password;
            }
          }
        }
      }
      vacm {
        access {
          group group-name {
            (default-context-prefix | context-prefix context-prefix) {
              security-model (any | usm | v1 | v2c) {
                security-level (authentication | none | privacy) {
                  notify-view view-name;
                  read-view view-name;
                  write-view view-name;
                }
              }
            }
          }
        }
        security-to-group {
          security-model (usm | v1 | v2c) {
            security-name security-name {
              group group-name;
            }
          }
        }
      }
    }
```

Hierarchy Level [edit snmp]

Release Information 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 SNMPv3.

The remaining statements are explained separately. See CLI Explorer.

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

Related Documentation
- Minimum SNMPv3 Configuration on a Device Running Junos OS on page 216

vacm

Syntax

```
vacm {
  access {
    group group-name {
      (default-context-prefix | context-prefix context-prefix){
        security-model (any | usm | v1 | v2c) {
          security-level (authentication | none | privacy) {
            notify-view view-name;
            read-view view-name;
            write-view view-name;
          }
        }
      }
    }
  }
  security-to-group {
    security-model (usm | v1 | v2c);
    security-name security-name {
      group group-name;
    }
  }
}
```

Hierarchy Level [edit snmp v3]

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

Description Configure view-based access control model (VACM) information.

The remaining statements are explained separately. See CLI Explorer.

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

Related Documentation
- *Defining Access Privileges for an SNMP Group*

 Copyright © 2018, Juniper Networks, Inc.

variable

Syntax variable *oid-variable*;

Hierarchy Level [edit snmp rmon alarm *index*]

Release Information 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 Set the object identifier (OID) of the MIB object (also called variable) to be monitored when you configure an SNMP RMON alarm. If the value of the monitored variable exceeds the configured rising threshold or falling threshold, an alarm is triggered and a corresponding event may be generated.

Options ***oid-variable***—OID of the MIB variable that is being monitored. The OID can be a dotted decimal (for example, **1.3.6.1.2.1.2.1.2.2.1.10.1**) or the name of the MIB object—for example, **ifInOctets.1**.

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

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Configuring RMON Alarms and Events on page 262
- Monitoring RMON MIB Tables on page 271
- Understanding RMON on page 217
- *Junos OS Network Management Configuration Guide*

version

Syntax version (all | v1 | v2);

Hierarchy Level [edit snmp trap-group *group-name*]

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

Description Specify the version number of SNMP traps.

Default **all**—Send an SNMPv1 and SNMPv2 trap for every trap condition.

Options **all**—Send an SNMPv1 and SNMPv2 trap for every trap condition.

v1—Send SNMPv1 traps only.

v2—Send SNMPv2 traps only.

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

Related Documentation

- Configuring SNMP Trap Groups on page 258

 Copyright © 2018, Juniper Networks, Inc.

view (Configuring a MIB View)

Syntax

```
view view-name {
   oid object-identifier (include | exclude);
}
```

Hierarchy Level

[edit snmp]

Release Information

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

Define a MIB view. A MIB view identifies a group of MIB objects. Each MIB object in a view has a common OID prefix. Each object identifier represents a subtree of the MIB object hierarchy. The **view** statement uses a view to specify a group of MIB objects on which to define access. To enable a view, you must associate the view with a community by including the **view** statement at the **[edit snmp community *community-name*]** hierarchy level.

NOTE: To remove an OID completely, use the **delete view all oid oid-number** command but omit the **include** parameter.

Options

view-name—Name of the view.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

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

Related Documentation

- Configuring MIB Views on page 261
- *Associating MIB Views with an SNMP User Group*
- community on page 300

view (Associating MIB View with a Community)

Syntax view *view-name*;

Hierarchy Level [edit snmp community *community-name*]

Release Information 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 Associate a view with a community. A view represents a group of MIB objects.

Options ***view-name***—Name of the view. You must use a view name already configured in the **view** statement at the **[edit snmp]** hierarchy level.

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

Related Documentation
- *Configuring SNMP Communities*

write-view

Syntax write-view *view-name*;

Hierarchy Level [edit snmp v3 vacm access group *group-name* (default-context-prefix | context-prefix *context-prefix*) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]

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 switches.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Associate the write view with a community (for SNMPv1 or SNMPv2c clients) or a group name (for SNMPv3 clients).

Options ***view-name***—Name of the view for which the SNMP user group has write permission.

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

Related Documentation
- Configuring MIB Views on page 261
- *Configuring the Write View*

 Copyright © 2018, Juniper Networks, Inc.

CHAPTER 15

SNMP Operational Commands

- clear snmp history
- clear snmp statistics
- request snmp spoof-trap
- request snmp utility-mib clear instance
- request snmp utility-mib set instance
- show snmp health-monitor
- show snmp inform-statistics
- show snmp mib
- show snmp rmon
- show snmp rmon history
- show snmp statistics
- show snmp v3

Copyright © 2018, Juniper Networks, Inc.

clear snmp history

Syntax clear snmp history (*index* | all)

Release Information Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Delete the samples of Ethernet statistics collected for a history group.

Options **all**—Clear all the entries in the history index.

index—Clear the contents of the specified entry in the history index.

Required Privilege Level clear

Related Documentation

- clear snmp statistics on page 387

 Copyright © 2018, Juniper Networks, Inc.

clear snmp statistics

Syntax clear snmp statistics

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 the OCX Series.

Description Clear Simple Network Management Protocol (SNMP) statistics.

Options This command has no options.

Required Privilege Level clear

Related Documentation
- show snmp statistics on page 412

List of Sample Output clear snmp statistics on page 387

Output Fields See show snmp statistics for an explanation of output fields.

Sample Output

clear snmp statistics

In the following example, SNMP statistics are displayed before and after the **clear snmp statistics** command is issued:

```
user@host> show snmp statistics
SNMP statistics:
  Input:
    Packets: 8, Bad versions: 0, Bad community names: 0,
    Bad community uses: 0, ASN parse errors: 0,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 8, Total set varbinds: 0,
    Get requests: 0, Get nexts: 8, Set requests: 0,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops 0
  Output:
    Packets: 2298, Too bigs: 0, No such names: 0,
    Bad values: 0, General errors: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 8, Traps: 2290

user@host> clear snmp statistics

user@host> show snmp statistics
```

```
SNMP statistics:
  Input:
    Packets: 0, Bad versions: 0, Bad community names: 0,
    Bad community uses: 0, ASN parse errors: 0,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 0, Total set varbinds: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops 0
  Output:
    Packets: 0, Too bigs: 0, No such names: 0,
    Bad values: 0, General errors: 0,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 0, Traps: 0
```


Copyright © 2018, Juniper Networks, Inc.

request snmp spoof-trap

Syntax

request snmp spoof-trap
<*trap*> **variable-bindings** <*object*> <*instance*> <*value*>

Release Information

Command introduced in Junos OS Release 8.2.
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 the OCX Series.

Description

Spoof (mimic) the behavior of a Simple Network Management Protocol (SNMP) trap.

Options

<*trap*>—Name of the trap to spoof.

variable-bindings <*object*> <*instance*> <*value*>—(Optional) List of variables and values to include in the trap. Each variable binding is specified as an object name, the object instance, and the value (for example, **ifIndex[14] = 14**). Enclose the list of variable bindings in quotation marks (" ") and use a comma to separate each object name, instance, and value definition (for example, **variable-bindings "ifIndex[14] = 14, ifAdminStatus[14] = 1, ifOperStatus[14] = 2"**). Objects included in the trap definition that do not have instances and values specified as part of the command are included in the trap and spoofed with automatically generated instances and values.

<*dummy name*>—A dummy trap name to display the list of available traps.

Question mark (?)—Question mark**?** to display possible completions.

Required Privilege Level

request

List of Sample Output

request snmp spoof-trap (with Variable Bindings) on page 389
request snmp spoof-trap (Illegal Trap Name) on page 389
request snmp spoof-trap (Question Mark ?) on page 394

Sample Output

request snmp spoof-trap (with Variable Bindings)

```
user@host> request snmp spoof-trap linkUp variable-bindings "ifIndex[14] = 14, ifAdminStatus[14]
= 1, ifOperStatus[14] = 2"
Spoof trap request result: trap sent successfully
```

request snmp spoof-trap (Illegal Trap Name)

```
user@host> request snmp spoof-trap xx
Spoof trap request result: trap not found

Allowed Traps:
adslAtucInitFailureTrap
  adslAtucPerfESsThreshTrap
  adslAtucPerfLofsThreshTrap
```

```
adslAtucPerfLolsThreshTrap
adslAtucPerfLossThreshTrap
adslAtucPerfLprsThreshTrap
adslAtucRateChangeTrap
adslAturPerfESsThreshTrap
adslAturPerfLofsThreshTrap
adslAturPerfLossThreshTrap
adslAturPerfLprsThreshTrap
adslAturRateChangeTrap
apsEventChannelMismatch
apsEventFEPLF
apsEventModeMismatch
apsEventPSBF
apsEventSwitchover
authenticationFailure
bfdSessDown
bfdSessUp
bgpBackwardTransition
bgpEstablished
coldStart
dlswTrapCircuitDown
dlswTrapCircuitUp
dlswTrapTConnDown
dlswTrapTConnPartnerReject
dlswTrapTConnProtViolation
dlswTrapTConnUp
dsx1LineStatusChange
dsx3LineStatusChange
entConfigChange
fallingAlarm
frDLCIStatusChange
ggsnTrapChanged
ggsnTrapCleared
ggsnTrapNew
gmplsTunnelDown
ifMauJabberTrap
ipv6IfStateChange
isisAreaMismatch
isisAttemptToExceedMaxSequence
isisAuthenticationFailure
isisAuthenticationTypeFailure
isisCorruptedLSPDetected
isisDatabaseOverload
isisIDLenMismatch
isisLSPTooLargeToPropagate
isisManualAddressDrops
isisMaxAreaAddressesMismatch
isisOriginatingLSPBufferSizeMismatch
isisOwnLSPPurge
isisProtocolsSupportedMismatch
isisRejectedAdjacency
isisSequenceNumberSkip
isisVersionSkew
jnxAccessAuthServerDisabled
jnxAccessAuthServerEnabled
jnxAccessAuthServiceDown
jnxAccessAuthServiceUp
jnxBfdSessDetectionTimeHigh
jnxBfdSessTxIntervalHigh
jnxBgpM2BackwardTransition
jnxBgpM2Established
```

 Copyright © 2018, Juniper Networks, Inc.

```
jnxCmCfgChange
jnxCmRescueChange
jnxCollFlowOverload
jnxCollFlowOverloadCleared
jnxCollFtpSwitchover
jnxCollMemoryAvailable
jnxCollMemoryUnavailable
jnxCollUnavailableDest
jnxCollUnavailableDestCleared
jnxCollUnsuccessfulTransfer
jnxDfcHardMemThresholdExceeded
jnxDfcHardMemUnderThreshold
jnxDfcHardPpsThresholdExceeded
jnxDfcHardPpsUnderThreshold
jnxDfcSoftMemThresholdExceeded
jnxDfcSoftMemUnderThreshold
jnxDfcSoftPpsThresholdExceeded
jnxDfcSoftPpsUnderThreshold
jnxEventTrap
jnxExampleStartup
jnxFEBSwitchover
jnxFanFailure
jnxFanOK
jnxFruCheck
jnxFruFailed
jnxFruInsertion
jnxFruOK
jnxFruOffline
jnxFruOnline
jnxFruPowerOff
jnxFruPowerOn
jnxFruRemoval
jnxHardDiskFailed
jnxHardDiskMissing
jnxJsAvPatternUpdateTrap
jnxJsChassisClusterSwitchover
jnxJsFwAuthCapacityExceeded
jnxJsFwAuthFailure
jnxJsFwAuthServiceDown
jnxJsFwAuthServiceUp
jnxJsNatAddrPoolThresholdStatus
jnxJsScreenAttack
jnxJsScreenCfgChange
jnxLdpLspDown
jnxLdpLspUp
jnxLdpSesDown
jnxLdpSesUp
jnxMIMstCistPortLoopProtectStateChangeTrap
jnxMIMstCistPortRootProtectStateChangeTrap
jnxMIMstErrTrap
jnxMIMstGenTrap
jnxMIMstInvalidBpduRxdTrap
jnxMIMstMstiPortLoopProtectStateChangeTrap
jnxMIMstMstiPortRootProtectStateChangeTrap
jnxMIMstNewRootTrap
jnxMIMstProtocolMigrationTrap
jnxMIMstRegionConfigChangeTrap
jnxMIMstTopologyChgTrap
jnxMacChangedNotification
jnxMplsLdpInitSesThresholdExceeded
jnxMplsLdpPathVectorLimitMismatch
```

```
jnxMplsLdpSessionDown
jnxMplsLdpSessionUp
jnxOspfv3IfConfigError
jnxOspfv3IfRxBadPacket
jnxOspfv3IfStateChange
jnxOspfv3LsdbApproachingOverflow
jnxOspfv3LsdbOverflow
jnxOspfv3NbrRestartHelperStatusChange
jnxOspfv3NbrStateChange
jnxOspfv3NssaTranslatorStatusChange
jnxOspfv3RestartStatusChange
jnxOspfv3VirtIfConfigError
jnxOspfv3VirtIfRxBadPacket
jnxOspfv3VirtIfStateChange
jnxOspfv3VirtNbrRestartHelperStatusChange
jnxOspfv3VirtNbrStateChange
jnxOtnAlarmCleared
jnxOtnAlarmSet
jnxOverTemperature
jnxPMonOverloadCleared
jnxPMonOverloadSet
jnxPingEgressJitterThresholdExceeded
jnxPingEgressStdDevThresholdExceeded
jnxPingEgressThresholdExceeded
jnxPingIngressJitterThresholdExceeded
jnxPingIngressStddevThresholdExceeded
jnxPingIngressThresholdExceeded
jnxPingRttJitterThresholdExceeded
jnxPingRttStdDevThresholdExceeded
jnxPingRttThresholdExceeded
jnxPortBpduErrorStatusChangeTrap
jnxPortLoopProtectStateChangeTrap
jnxPortRootProtectStateChangeTrap
jnxPowerSupplyFailure
jnxPowerSupplyOK
jnxRedundancySwitchover
jnxRmonAlarmGetFailure
jnxRmonGetOk
jnxSecAccessIfMacLimitExceeded
jnxSecAccessdsRateLimitCrossed
jnxSonetAlarmCleared
jnxSonetAlarmSet
jnxSpSvcSetCpuExceeded
jnxSpSvcSetCpuOk
jnxSpSvcSetZoneEntered
jnxSpSvcSetZoneExited
jnxStormEventNotification
jnxSyslogTrap
jnxTemperatureOK
jnxVccpPortDown
jnxVccpPortUp
jnxVpnIfDown
jnxVpnIfUp
jnxVpnPwDown
jnxVpnPwUp
jnxl2aldGlobalMacLimit
jnxl2aldInterfaceMacLimit
jnxl2aldRoutingInstMacLimit
linkDown
linkUp
lldpRemTablesChange
```


Copyright © 2018, Juniper Networks, Inc.

```
mfrMibTrapBundleLinkMismatch
mplsLspChange
mplsLspDown
mplsLspInfoChange
mplsLspInfoDown
mplsLspInfoPathDown
mplsLspInfoPathUp
mplsLspInfoUp
mplsLspPathDown
mplsLspPathUp
mplsLspUp
mplsNumVrfRouteMaxThreshExceeded
mplsNumVrfRouteMidThreshExceeded
mplsNumVrfSecIllglLblThrshExcd
mplsTunnelDown
mplsTunnelReoptimized
mplsTunnelRerouted
mplsTunnelUp
mplsVrfIfDown
mplsVrfIfUp
mplsXCDown
mplsXCUp
msdpBackwardTransition
msdpEstablished
newRoot
ospfIfAuthFailure
ospfIfConfigError
ospfIfRxBadPacket
ospfIfStateChange
ospfLsdbApproachingOverflow
ospfLsdbOverflow
ospfMaxAgeLsa
ospfNbrStateChange
ospfOriginateLsa
ospfTxRetransmit
ospfVirtIfAuthFailure
ospfVirtIfConfigError
ospfVirtIfRxBadPacket
ospfVirtIfStateChange
ospfVirtIfTxRetransmit
ospfVirtNbrStateChange
pethMainPowerUsageOffNotification
pethMainPowerUsageOnNotification
pethPsePortOnOffNotification
pingProbeFailed
pingTestCompleted
pingTestFailed
ptopoConfigChange
risingAlarm
rpMauJabberTrap
sdlcLSStatusChange
sdlcPortStatusChange
topologyChange
traceRoutePathChange
traceRouteTestCompleted
traceRouteTestFailed
vrrpTrapAuthFailure
vrrpTrapNewMaster
warmStart
```

request snmp spoof-trap (Question Mark ?)

```
user@host> request snmp spoof-trap ?
Possible completions:
  <trap>               The name of the trap to spoof
  adslAtucInitFailureTrap
  adslAtucPerfESsThreshTrap
  adslAtucPerfLofsThreshTrap
  adslAtucPerfLolsThreshTrap
  adslAtucPerfLossThreshTrap
  adslAtucPerfLprsThreshTrap
  adslAtucRateChangeTrap
  adslAturPerfESsThreshTrap
  adslAturPerfLofsThreshTrap
  adslAturPerfLossThreshTrap
  adslAturPerfLprsThreshTrap
  adslAturRateChangeTrap
  apsEventChannelMismatch
  apsEventFEPLF
  apsEventModeMismatch
  apsEventPSBF
  apsEventSwitchover
  authenticationFailure
  bfdSessDown
  bfdSessUp
  bgpBackwardTransition
  bgpEstablished
  coldStart
  dlswTrapCircuitDown
  dlswTrapCircuitUp
---(more 10%)---
```


Copyright © 2018, Juniper Networks, Inc.

request snmp utility-mib clear instance

Syntax

request snmp utility-mib clear instance *name*
object-type *type*

Release Information

Command introduced in Junos OS Release 12.2 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Clear the data stored in the specified container object in the SNMP Utility MIB.

Options

name—Name of the SNMP instance that is used to identify the data stored in the container object.

object-type *type*—Type of container object in which the data is stored. The following container object types are supported:

- **counter**—Stores a 32-bit counter value.
- **counter64**—Stores a 64-bit counter value.
- **integer**—Stores a 32-bit signed integer value.
- **unsigned-integer**—Stores a 32-bit unsigned integer value.

Required Privilege Level

clear

Related Documentation

- Utility MIB on page 214
- *Understanding the Implementation of SNMP on the QFabric System*
- **request snmp utility-mib set instance on page 396**

request snmp utility-mib set instance

Syntax

request snmp utility-mib set instance *name*
object-type *type*
object-value *value*

Release Information

Command introduced in Junos OS Release 12.2 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Store data in the specified container object in the SNMP Utility MIB. The data may be retrieved by SNMP operations.

Options

name—Name of the SNMP instance that is used to identify the data stored in the container object.

object-type *type*—Type of container object in which to store data. The following container object types are supported:

- **counter**—Stores a 32-bit counter value.
- **counter64**—Stores a 64-bit counter value.
- **integer**—Stores a 32-bit signed integer value.
- **unsigned-integer**—Stores a 32-bit unsigned integer value.
- **string**—Stores an octet string value.

object-value *value*—Data that is stored in the container object.

Required Privilege Level

request

Related Documentation

- Utility MIB on page 214
- *Understanding the Implementation of SNMP on the QFabric System*
- **request snmp utility-mib clear instance on page 395**

Copyright © 2018, Juniper Networks, Inc.

show snmp health-monitor

Syntax

show snmp health-monitor
<alarms (brief | detail) | logs>

Release Information

Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Display information about Simple Network Management Protocol (SNMP) health monitor alarms and logs.

Options

none—Display information about all health monitor alarms and logs.

alarms (brief | detail)—(Optional) Display information about health monitor alarms. Optionally, specify brief or detailed information about the alarms.

logs—(Optional) Display information about health monitor logs.

Required Privilege Level

view

Related Documentation

- Understanding Health Monitoring on page 221
- Configuring Health Monitoring on page 265

List of Sample Output

show snmp health-monitor on page 399
show snmp health-monitor alarms detail on page 399

Output Fields

Table 49 on page 397 describes the output fields for the **show snmp health-monitor** command. Output fields are listed in the approximate order in which they appear.

Table 49: show snmp health-monitor Output Fields

Field Name	Field Description	Level of Output
Alarm Index	Alarm identifier.	All levels
Variable description	Description of the health monitor object instance being monitored.	All levels
Variable name	Name of the health monitor object instance being monitored.	All levels
Value	Current value of the monitored variable in the most recent sample interval.	All levels

Table 49: show snmp health-monitor Output Fields *(continued)*

Field Name	Field Description	Level of Output

State	State of the alarm or event entry:
	• Alarms:
	  • active—Entry is fully configured and activated.
	  • falling threshold crossed—Value of the variable has crossed the lower threshold limit.
	  • rising threshold crossed—Value of the variable has crossed the upper threshold limit.
	  • under creation—Entry is being configured and is not yet activated.
	  • startup—Alarm is waiting for the first sample of the monitored variable.
	  • object not available—Monitored variable of that type is not available to the health monitor agent.
	  • instance not available—Monitored variable's instance is not available to the health monitor agent.
	  • object type invalid—Monitored variable is not a numeric value.
	  • object processing errored—An error occurred when the monitored variable was processed.
	  • unknown—State is not one of the above.
		All levels

Variable OID	Object ID to which the variable name is resolved. The format is x.x.x.x.	detail
Sample type	Method of sampling the monitored variable and calculating the value to compare against the upper and lower thresholds. It can have the value *absolute value* or *delta value*.	detail

Startup alarm	Alarm that might be sent when this entry is first activated, depending on the following criteria:
	• Alarm is sent when one of the following situations exists:
	  • Value of the alarm is above or equal to the rising threshold and the startup type is either rising alarm or rising or falling alarm. *falling alarm*
	  • Value of the alarm is below or equal to the falling threshold and the startup type is either *falling alarm* or *rising or falling alarm*.
	• Alarm is *not* sent when one of the following situations exists:
	  • Value of the alarm is above or equal to the rising threshold and the startup type is *falling alarm*.
	  • Value of the alarm is below or equal to the falling threshold and the startup type is *rising alarm*.
	  • Value of the alarm is between the thresholds.
		detail

Owner	Name of the entry configured by the user. If the entry was created through the CLI, the owner has **monitor** prepended to it.	detail
Creator	Mechanism by which the entry was configured (Health Monitor).	detail
Sample interval	Time period between samples (in seconds).	detail
Rising threshold	Upper limit threshold value as a percentage of the maximum possible value.	detail

Copyright © 2018, Juniper Networks, Inc.

Table 49: show snmp health-monitor Output Fields *(continued)*

Field Name	Field Description	Level of Output
Falling threshold	Lower limit threshold value as a percentage of the maximum possible value.	detail
Rising event index	Index number of the event triggered when the rising threshold is crossed.	detail
Falling event index	Index number of the event triggered when the falling threshold is crossed. Details include the value of the falling event instance and the state of the falling event instance.	detail

Sample Output

show snmp health-monitor

```
user@switch> show snmp health-monitor

Alarm
Index  Variable description                          Value State

 32768 Health Monitor: root file system utilization
       jnxHrStoragePercentUsed.1                       59 active


 32769 Health Monitor: /config file system utilization
       jnxHrStoragePercentUsed.2                        0 active


 32770 Health Monitor: RE 0 CPU utilization
       jnxOperatingCPU.9.1.0.0                          9 falling threshold


 32772 Health Monitor: RE 0 memory utilization
       jnxOperatingBuffer.9.1.0.0                      23 active


 32774 Health Monitor: Max Kernel Memory Used (%)
       jnxBoxKernelMemoryUsedPercent.0                  3 active
Event Index: 32768
    Description: Health Monitor: RE 0 CPU utilization crossed falling threshold
70 (value: 5), (variable: jnxOperatingCPU.9.1.0.0)
    Time: 2011-01-09 19:18:35 PST
```

show snmp health-monitor alarms detail

```
user@switch> show snmp health-monitor alarms detail

Alarm Index 32768:
  Variable name                       jnxHrStoragePercentUsed.1
  Variable OID                        1.3.6.1.4.1.2636.3.31.1.1.1.1.1
  Sample type                         absolute value
  Startup alarm                       rising alarm
  Owner                               Health Monitor: root file system
                                      utilization
  Creator                             Health Monitor
  State                               active
  Sample interval                 300 seconds
```

```
  Rising threshold                 80
  Falling threshold                70
  Rising event index            32768
  Falling event index           32768
    Instance Value: 59
    Instance State: active

Alarm Index 32769:
  Variable name                       jnxHrStoragePercentUsed.2
  Variable OID                        1.3.6.1.4.1.2636.3.31.1.1.1.1.2
  Sample type                         absolute value
  Startup alarm                       rising alarm
  Owner                               Health Monitor: /config file system
                                      utilization
  Creator                             Health Monitor
  State                               active
  Sample interval                 300 seconds
  Rising threshold                 80
  Falling threshold                70
  Rising event index            32768
  Falling event index           32768
    Instance Value: 0
    Instance State: active

Alarm Index 32770:
  Variable name                       jnxOperatingCPU.9.1.0.0
  Variable OID                        1.3.6.1.4.1.2636.3.1.13.1.8.9.1.0.0
  Sample type                         absolute value
  Startup alarm                       rising alarm
  Owner                               Health Monitor: RE 0 CPU utilization

  Creator                             Health Monitor
  State                               active
  Sample interval                 300 seconds
  Rising threshold                 80
  Falling threshold                70
  Rising event index            32768
  Falling event index           32768
    Instance Value: 9
    Instance State: falling threshold

Alarm Index 32772:
  Variable name                       jnxOperatingBuffer.9.1.0.0
  Variable OID                        1.3.6.1.4.1.2636.3.1.13.1.11.9.1.0.0
  Sample type                         absolute value
  Startup alarm                       rising alarm
  Owner                               Health Monitor: RE 0 memory utilization

  Creator                             Health Monitor
  State                               active
  Sample interval                 300 seconds
  Rising threshold                 80
  Falling threshold                70
  Rising event index            32768
  Falling event index           32768
    Instance Value: 23
    Instance State: active

Alarm Index 32774:
  Variable name                       jnxBoxKernelMemoryUsedPercent.0
  Variable OID                        1.3.6.1.4.1.2636.3.1.16.0
```

 Copyright © 2018, Juniper Networks, Inc.

```
Sample type                          absolute value
Startup alarm                        rising alarm
Owner                                Health Monitor: Max Kernel Memory Used
                                     (%)
Creator                              Health Monitor
State                                active
Sample interval                  300 seconds
Rising threshold                  80
Falling threshold                 70
Rising event index            32768
Falling event index           32768
  Instance Value: 3
  Instance State: active
```

show snmp inform-statistics

Syntax show snmp inform-statistics

Release Information Command introduced in 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 the OCX Series.

Description Display information about Simple Network Management Protocol (SNMP) inform requests.

Options This command has no options.

Required Privilege Level view

List of Sample Output show snmp inform-statistics on page 402

Output Fields Table 50 on page 402 describes the output fields for the **show snmp inform-statistics** command. Output fields are listed in the approximate order in which they appear.

Table 50: show snmp inform-statistics Output Fields

Field Name	Field Description
Target Name	Name of the device configured to receive and respond to SNMP informs.
Address	IP address of the target device.
Sent	Number of informs sent to the target device and acknowledged by the target device.
Pending	Number of informs held in memory pending a response from the target device.
Discarded	Number of informs discarded after the specified number of retransmissions to the target device were attempted.
Timeouts	Number of informs that did not receive an acknowledgement from the target device within the timeout specified.
Probe Failures	Connection failures that occurred (for example, when the target server returned invalid content or you incorrectly configured the target address).

Sample Output

show snmp inform-statistics

```
user@host> show snmp inform-statistics
```

 Copyright © 2018, Juniper Networks, Inc.

```
Inform Request Statistics:
 Target Name: TA1_v3_md5_none Address: 172.17.20.184
  Sent: 176, Pending: 0
  Discarded: 0, Timeouts: 0, Probe Failures: 0
 Target Name: TA2_v3_sha_none Address: 192.168.110.59
  Sent: 0, Pending: 4
  Discarded: 84, Timeouts: 0, Probe Failures: 258
 Target Name: TA5_v2_none Address: 172.17.20.184
  Sent: 0, Pending: 0
  Discarded: 2, Timeouts: 10, Probe Failures: 0
```

show snmp mib

Syntax show snmp mib (get | get-next | walk) (ascii | decimal) *object-id*

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
ascii and **decimal** options introduced in Junos OS Release 9.6.
ascii and **decimal** options introduced in Junos OS Release 9.6 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 the OCX Series.

Description Display local Simple Network Management Protocol (SNMP) Management Information Base (MIB) object values.

Options

get—Retrieve and display one or more SNMP object values.

get-next—Retrieve and display the next SNMP object values.

walk—Retrieve and display the SNMP object values that are associated with the requested object identifier (OID). When you use this option, the Junos OS displays the objects below the subtree that you specify.

ascii—Display the SNMP object's string indices as an ASCII-key representation.

decimal—Display the SNMP object values in the decimal (default) format. The **decimal** option is the default option for this command. Therefore, issuing the **show snmp mib (get | get-next | walk) decimal object-id** and the **show snmp mib (get | get-next | walk) object-id** commands display the same output.

object-id—The object can be represented by a sequence of dotted integers (such as **1.3.6.1.2.1.2**) or by its subtree name (such as **interfaces**). When entering multiple objects, enclose the objects in quotation marks.

Required Privilege Level **snmp**—To view this statement in the configuration.

List of Sample Output

show snmp mib get on page 405
show snmp mib get (Multiple Objects) on page 405
show snmp mib get (Layer 2 Policer) on page 405
show snmp mib get-next on page 405
show snmp mib get-next (Specify an OID) on page 405
show snmp mib walk on page 405
show snmp mib walk (QFX Series) on page 406
show snmp mib walk decimal on page 406
show snmp mib walk (ASCII) on page 406
show snmp mib walk (Multiple Indices) on page 406
show snmp mib walk decimal (Multiple Indices) on page 406

 Copyright © 2018, Juniper Networks, Inc.

Output Fields Table 51 on page 405 describes the output fields for the **show snmp mib** command. Output fields are listed in the approximate order in which they appear.

Table 51: show snmp mib Output Fields

Field Name	Field Description
name	Object name and numeric instance value.
object value	Object value. The Junos OS translates OIDs into the corresponding object names.

Sample Output

show snmp mib get

```
user@host> show snmp mib get sysObjectID.0
sysObjectID.0 = jnxProductNameM20
```

show snmp mib get (Multiple Objects)

```
user@host> show snmp mib get "sysObjectID.0 sysUpTime.0"
sysObjectID.0 = jnxProductNameM20
sysUpTime.0 = 1640992
```

show snmp mib get (Layer 2 Policer)

```
user@host> show snmp mib get ifInOctets.25970
ifInOctets.25970 = 7545720
```

show snmp mib get-next

```
user@host> show snmp mib get-next jnxMibs
jnxBoxClass.0 = jnxProductLineM20.0
```

show snmp mib get-next (Specify an OID)

```
user@host> show snmp mib get-next 1.3.6.1
sysDescr.0    = Juniper Networks, Inc. m20 internet router, kernel
Junos OS Release: 2004-1 Build date: build date UTC Copyright (c) 1996-2004 Juniper
 Networks, Inc.
```

show snmp mib walk

```
user@host> show snmp mib walk system
sysDescr.0    = Juniper Networks, Inc. m20 internet router, kernel
Junos OS Release #0: 2004-1 Build date: build date UTC Copyright (c) 1996-2004
Juniper Networks, Inc.
sysObjectID.0 = jnxProductNameM20
sysUpTime.0 = 1640992
sysContact.0 = Your contact
sysName.0 = my router
sysLocation.0 = building 1
sysServices.0 = 4
```

Copyright © 2018, Juniper Networks, Inc.

show snmp mib walk (QFX Series)

```
user@switch> show snmp mib walk system
sysDescr.0    = Juniper Networks, Inc. qfx3500s internet router, kernel JUNOS
11.1-20100926.0 #0: 2010-09-26 06:17:38 UTC Build date: 2010-09-26 06:00:10
sysObjectID.0 = jnxProductQFX3500
sysUpTime.0   = 138980301
sysContact.0  = System Contact
sysName.0     = LabQFX3500
sysLocation.0 = Lab
sysServices.0 = 4
```

show snmp mib walk decimal

```
user@host show snmp mib walk decimal jnxUtilData
jnxUtilCounter32Value.102.114.101.100 = 100
```

show snmp mib walk (ASCII)

```
show snmp mib walk ascii jnxUtilData
jnxUtilCounter32Value."fred" = 100
```

show snmp mib walk (Multiple Indices)

```
show snmp mib walk ascii jnxFWCounterByteCount
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_BE-fe-1/3/0.0-i".2 = 0
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_CC-fe-1/3/0.0-i".2 = 0
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_RT-fe-1/3/0.0-i".2 = 0
.......
```

show snmp mib walk decimal (Multiple Indices)

```
show snmp mib walk ascii jnxFWCounterByteCount
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_BE-fe-1/3/0.0-i".2 = 0
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_CC-fe-1/3/0.0-i".2 = 0
jnxFWCounterByteCount."fe-1/3/0.0-i"."CLASS_RT-fe-1/3/0.0-i".2 = 0
.......
```


Copyright © 2018, Juniper Networks, Inc.

show snmp rmon

Syntax

show snmp rmon
<alarms (brief | detail)>
<events (brief | detail)>
<logs>

Release Information

Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Display information about Simple Network Management Protocol (SNMP) Remote Monitoring (RMON) alarms, events, and logs.

Options

none—Display information about all RMON alarms and events.

brief | detail—(Optional) Display brief or detailed information about RMON alarms or events.

alarms—(Optional) Display information about RMON alarms.

events—(Optional) Display information about RMON events.

logs—(Optional) Display information about RMON monitoring logs.

Required Privilege Level

view

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Monitoring RMON MIB Tables on page 271
- Configuring RMON Alarms and Events on page 262
- Understanding RMON on page 217
- **clear snmp statistics on page 387**
- **clear snmp history on page 386**
- **show snmp rmon history on page 411**

List of Sample Output

show snmp rmon on page 409
show snmp rmon alarms detail on page 410
show snmp rmon events detail on page 410
show snmp rmon logs on page 410

Output Fields

Table 52 on page 408 describes the output fields for the **show snmp rmon** command. Output fields are listed in the approximate order in which they appear.

Table 52: show snmp rmon Output Fields

Field Name	Field Description	Level of Output
Alarm Index	Alarm identifier.	All levels
State	State of the alarm or event entry: Alarms: • **active**—Entry is fully configured and activated. • **falling threshold crossed**—Value of the variable has crossed the lower threshold limit. • **rising threshold crossed**—Value of the variable has crossed the upper threshold limit. • **under creation**—Entry is being configured and is not yet activated. • **startup**—Alarm is waiting for the first sample of the monitored variable. • **object not available**—Monitored variable of that type is not available to the SNMP agent. • **instance not available**—Monitored variable's instance is not available to the SNMP agent. • **object type invalid**—Monitored variable is not a numeric value. • **object processing errored**—An error occurred when the monitored variable was processed. • **unknown**—State is not one of the above. Events: • **active**—Entry has been fully configured and activated. • **under creation**—Entry is being configured and is not yet activated. • **unknown**—State is not one of the above.	All levels
Variable name	Name of the SNMP object instance being monitored.	All levels
Event Index	Event identifier.	All levels
Type	Type of notification made when an event is triggered. It can be one of the following: • **log**—A system log message is generated and an entry is made to the log table. • **snmptrap**—An SNMP trap is sent to the configured destination. • **log and trap**—A system log message is generated, an entry is made to the log table, and an SNMP trap is sent to the configured destination. • **none**—Neither log nor trap will be sent.	**detail**
Last Event	Date and time of the last event. It has the format *yyyy-mm-dd hh:mm:ss timezone*.	**brief**
Community	Trap group used for sending the SNMP trap.	**detail**
Variable OID	Object ID to which the variable name is resolved. The format is **x.x.x.x**.	**detail**

Copyright © 2018, Juniper Networks, Inc.

Table 52: show snmp rmon Output Fields *(continued)*

Field Name	Field Description	Level of Output
Sample type	Method of sampling the monitored variable and calculating the value to compare against the upper and lower thresholds. It can have the value of **absolute value** or **delta value**.	**detail**

Startup alarm	Alarm that might be sent when this entry is first activated, depending on the following criteria:
	• Alarm is sent when one of the following situations exists:
	  ◦ Value of the alarm is above or equal to the rising threshold and the startup type is either **rising alarm** or **rising or falling alarm.**
	  ◦ Value of the alarm is below or equal to the falling threshold and the startup type is either **falling alarm** or **rising or falling alarm**.
	• Alarm is *not* sent when one of the following situations exists:
	  ◦ Value of the alarm is above or equal to the rising threshold and the startup type is **falling alarm**.
	  ◦ Value of the alarm is below or equal to the falling threshold and the startup type is **rising alarm**.
	  ◦ Value of the alarm is between the thresholds.
		detail

Owner	Name of the entry configured by the user. If the entry was created through the CLI, the owner has **monitor** prepended to it.	**detail**
Creator	Mechanism by which the entry was configured (**CLI** or **SNMP**).	**detail**
Sample interval	Time period between samples (in seconds).	**detail**
Rising threshold	Upper limit threshold value configured by the user.	**detail**
Falling threshold	Lower limit threshold value configured by the user.	**detail**
Rising event index	Event triggered when the rising threshold is crossed.	**detail**
Falling event index	Event triggered when the falling threshold is crossed.	**detail**
Current value	Current value of the monitored variable in the most recent sample interval.	**detail**

Sample Output

show snmp rmon

```
user@host> show snmp rmon
Alarm
Index  Variable description                          Value State

     5 monitor
       jnxOperatingCPU.9.1.0.0                           5 falling threshold

Event
Index  Type                        Last Event
```

```
    1  log and trap                2009-07-10 11:34:17 PDT
Event Index: 1
    Description: Event 1 triggered by Alarm 5, rising threshold (90) crossed,
(variable: jnxOperatingCPU.9.1.0.0, value: 100)
    Time: 2009-07-10 11:34:07 PDT
    Description: Event 1 triggered by Alarm 5, falling threshold (75) crossed,
(variable: jnxOperatingCPU.9.1.0.0, value: 5)
    Time: 2009-07-10 11:34:17 PDT
```

show snmp rmon alarms detail

```
user@host> show snmp rmon alarms detail
Alarm Index 5:
  Variable name                        jnxOperatingCPU.9.1.0.0
  Variable OID                         1.3.6.1.4.1.2636.3.1.13.1.8.9.1.0.0
  Sample type                          absolute value
  Startup alarm                        rising or falling alarm
  Owner                                monitor

  Creator                              CLI
  State                                active
  Sample interval                    5 seconds
  Rising threshold                  90
  Falling threshold                 75
  Rising event index                 1
  Falling event index                1
    Instance Value: 4
    Instance State: falling threshold
```

show snmp rmon events detail

```
user@host> show snmp rmon events detail
Event Index 1:
  Description                          rmon event
  Type                                 log and trap
  Community                            rmon-trap-group
  Last event                           2009-07-10 11:34:17 PDT
  Creator                              CLI
  State                                active
```

show snmp rmon logs

```
user@host> show snmp rmon logs
Event Index: 1
    Description: Event 1 triggered by Alarm 5, rising threshold (90) crossed,
(variable: jnxOperatingCPU.9.1.0.0, value: 100)
    Time: 2009-07-10 11:34:07 PDT
    Description: Event 1 triggered by Alarm 5, falling threshold (75) crossed,
(variable: jnxOperatingCPU.9.1.0.0, value: 5)
    Time: 2009-07-10 11:34:17 PDT
```


Copyright © 2018, Juniper Networks, Inc.

show snmp rmon history

Syntax

show snmp rmon history
<*history-index*>
sample-index <*sample-index*>

Release Information

Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Display the contents of the RMON history group.

Options

none—Display all the entries in the RMON history group.

history-index—(Optional) Display the contents of the specified entry in the RMON history group.

sample-index *sample-index*—(Optional) Display the statistics collected for the specified sample within the specified entry in the RMON history group.

Required Privilege Level

view

Related Documentation

- RMON MIB Event, Alarm, Log, and History Control Tables on page 219
- Monitoring RMON MIB Tables on page 271
- Configuring RMON Alarms and Events on page 262
- Understanding RMON on page 217
- **clear snmp statistics on page 387**
- **clear snmp history on page 386**
- **show snmp rmon on page 407**

Copyright © 2018, Juniper Networks, Inc.

show snmp statistics

Syntax

show snmp statistics
<subagents>

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.
Option **subagents** introduced in Junos OS Release 14.2.

Description

Display statistics about Simple Network Management Protocol (SNMP) packets sent and received by the router or switch.

Options

subagents—(Optional) Display the statistics of the protocol data unit (PDU), the number of SNMP requests and responses per subagent, and the SNMP statistics received from each subagent per logical system.

Required Privilege Level

view

Related Documentation

- clear snmp statistics on page 387

List of Sample Output

show snmp statistics on page 417
show snmp statistics subagents on page 417

Output Fields

Table 53 on page 413 describes the output fields for the **show snmp statistics** command. Output fields are listed in the approximate order in which they appear.

Copyright © 2018, Juniper Networks, Inc.

Table 53: show snmp statistics Output Fields

Field Name	Field Description
Input	Information about received packets: • **Packets(snmpInPkts)**—Total number of messages delivered to the SNMP entity from the transport service. • **Bad versions—(snmpInBadVersions**) Total number of messages delivered to the SNMP entity that were for an unsupported SNMP version. • **Bad community names—(snmpInBadCommunityNames)** Total number of messages delivered to the SNMP entity that used an SNMP community name not known to the entity. • **Bad community uses—(snmpInBadCommunityUses)** Total number of messages delivered to the SNMP entity that represented an SNMP operation that was not allowed by the SNMP community named in the message. • **ASN parse errors—(snmpInASNParseErrs)** Total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages. • **Too bigs—(snmpInTooBigs)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **tooBig**. • **No such names—(snmpInNoSuchNames)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **noSuchName**. • **Bad values—(snmpInBadValues)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **badValue**. • **Read onlys—(snmpInReadOnlys)** Total number of valid SNMP PDUs delivered to the SNMP entity with an error status field of **readOnly**. Only incorrect implementations of SNMP generate this error.

Table 53: show snmp statistics Output Fields *(continued)*

Field Name	Field Description
Input (continued)	• **General errors—(snmpInGenErrs)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **genErr**. • **Total requests varbinds—(snmpInTotalReqVars)** Total number of MIB objects retrieved successfully by the SNMP entity as a result of receiving valid SNMP **GetRequest** and **GetNext** PDUs. • **Total set varbinds—(snmpInSetVars)** Total number of MIB objects modified successfully by the SNMP entity as a result of receiving valid SNMP **SetRequest** PDUs. • **Get requests—(snmpInGetRequests)** Total number of SNMP **GetRequest** PDUs that have been accepted and processed by the SNMP entity. • **Get nexts—(snmpInGetNexts)** Total number of SNMP **GetNext** PDUs that have been accepted and processed by the SNMP entity. • **Set requests—(snmpInSetRequests)** Total number of SNMP **SetRequest** PDUs that have been accepted and processed by the SNMP entity. • **Get responses—(snmpInGetResponses)** Total number of SNMP **GetResponse** PDUs that have been accepted and processed by the SNMP entity. • **Traps—(snmpInTraps)** Total number of SNMP traps generated by the SNMP entity. • **Silent drops—(snmpSilentDrops)** Total number of **GetRequest**, **GetNextRequest**, **GetBulkRequest**, **SetRequests**, and **InformRequest** PDUs delivered to the SNMP entity that were silently dropped because the size of a reply containing an alternate response PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the requests. • **Proxy drops—(snmpProxyDrops)** Total number of **GetRequest**, **GetNextRequest**, **GetBulkRequest**, **SetRequests**, and **InformRequest** PDUs delivered to the SNMP entity that were silently dropped because the transmission of the message to a proxy target failed in such a way (other than a timeout) that no response PDU could be returned. • **Commit pending drops**—Number of SNMP packets for **Set** requests dropped because of a previous pending SNMP **Set** request on the committed configuration. • **Throttle drops**—Number of SNMP packets for any requests dropped reaching the throttle limit.

Copyright © 2018, Juniper Networks, Inc.

Table 53: show snmp statistics Output Fields *(continued)*

Field Name	Field Description
V3 Input	Information about SNMP version 3 packets: • **Unknown security models—(snmpUnknownSecurityModels)** Total number of packets received by the SNMP engine that were dropped because they referenced a security model that was not known to or supported by the SNMP engine. • **Invalid messages—(snmpInvalidMsgs)** Number of packets received by the SNMP engine that were dropped because there were invalid or inconsistent components in the SNMP message. • **Unknown pdu handlers—(snmpUnknownPDUHandlers)** Number of packets received by the SNMP engine that were dropped because the PDU contained in the packet could not be passed to an application responsible for handling the PDU type. • **Unavailable contexts—(snmpUnavailableContexts)** Number of requests received for a context that is known to the SNMP engine, but is currently unavailable. • **Unknown contexts—(snmpUnknownContexts)** Total number of requests received for a context that is unknown to the SNMP engine. • **Unsupported security levels—(usmStatsUnsupportedSecLevels)** Total number of packets received by the SNMP engine that were dropped because they requested a security level unknown to the SNMP engine (or otherwise unavailable). • **Not in time windows—(usmStatsNotInTimeWindows)** Total number of packets received by the SNMP engine that were dropped because they appeared outside the authoritative SNMP engine's window. • **Unknown user names—(usmStatsUnknownUserNames)** Total number of packets received by the SNMP engine that were dropped because they referenced a user that was not known to the SNMP engine. • **Unknown engine ids—(usmStatsUnknownEngineIDs)** Total number of packets received by the SNMP engine that were dropped because they referenced an SNMP engine ID that was not known to the SNMP engine. • **Wrong digests—(usmStatsWrongDigests)** Total number of packets received by the SNMP engine that were dropped because they did not contain the expected digest value. • **Decryption errors—(usmStatsDecryptionErrors)** Total number of packets received by the SNMP engine that were dropped because they could not be decrypted.

Table 53: show snmp statistics Output Fields *(continued)*

Field Name	Field Description
Output	Information about transmitted packets: • **Packets—(snmpOutPkts)** Total number of messages passed from the SNMP entity to the transport service. • **Too bigs—(snmpOutTooBigs)** Total number of SNMP PDUs generated by the SNMP entity with an error status field of **tooBig**. • **No such names—(snmpOutNoSuchNames)** Total number of SNMP PDUs delivered to the SNMP entity with an error status field of **noSuchName**. • **Bad values—(snmpOutBadValues)** Total number of SNMP PDUs generated by the SNMP entity with an error status field of **badValue**. • **General errors—(snmpOutGenErrs)** Total number of SNMP PDUs generated by the SNMP entity with an error status field of **genErr**. • **Get requests—(snmpOutGetRequests)** Total number of SNMP **GetRequest** PDUs generated by the SNMP entity. • **Get nexts—(snmpOutGetNexts)** Total number of SNMP **GetNext** PDUs generated by the SNMP entity. • **Set requests—(snmpOutSetRequests)** Total number of SNMP **SetRequest** PDUs generated by the SNMP entity. • **Get responses—(snmpOutGetResponses)** Total number of SNMP **GetResponse** PDUs generated by the SNMP entity. • **Traps—(snmpOutTraps)** Total number of SNMP traps generated by the SNMP entity.

Table 54 on page 416 describes the output fields for the **show snmp statistics subagents** command. Output fields are listed in the approximate order in which they appear.

Table 54: show snmp statistics subagents Output Fields

Field Name	Field Description
Subagent	Location of the SNMP subagent.
Request PDUs	Number of PDUs requested by the SNMP manager.
Response PDUs	Number of response PDUs sent by the SNMP subagent.
Request Variables	Number of variable bindings on the PDUs requested by the SNMP manager.
Response Variables	Number of variable bindings on the PDUs sent by the SNMP subagent.
Average Response Time	Average time taken by the SNMP subagent to send statistics response.
Maximum Response Time	Maximum time taken by the SNMP subagent to send the statistics response.

Copyright © 2018, Juniper Networks, Inc.

Sample Output

show snmp statistics

```
user@host> show snmp statistics
SNMP statistics:
  Input:
    Packets: 246213, Bad versions: 12, Bad community names: 12,
    Bad community uses: 0, ASN parse errors: 96,
    Too bigs: 0, No such names: 0, Bad values: 0,
    Read onlys: 0, General errors: 0,
    Total request varbinds: 227084, Total set varbinds: 67,
    Get requests: 44942, Get nexts: 190371, Set requests: 10712,
    Get responses: 0, Traps: 0,
    Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
    Throttle drops: 0,
  V3 Input:
    Unknown security models: 0, Invalid messages: 0
    Unknown pdu handlers: 0, Unavailable contexts: 0
    Unknown contexts: 0, Unsupported security levels: 1
    Not in time windows: 0, Unknown user names: 0
    Unknown engine ids: 44, Wrong digests: 23, Decryption errors: 0
  Output:
    Packets: 246093, Too bigs: 0, No such names: 31561,
    Bad values: 0, General errors: 2,
    Get requests: 0, Get nexts: 0, Set requests: 0,
    Get responses: 246025, Traps: 0
```

show snmp statistics subagents

```
user@host> show snmp statistics subagents

  Subagent: /var/run/cosd-20
    Request PDUs: 0, Response PDUs: 0,
    Request Variables: 0, Response Variables: 0,
    Average Response Time(ms): 0.00,
    Maximum Response Time(ms): 0.00

  Subagent: /var/run/pfed-30
    Request PDUs: 0, Response PDUs: 0,
    Request Variables: 0, Response Variables: 0,
    Average Response Time(ms): 0.00,
    Maximum Response Time(ms): 0.00

  Subagent: /var/run/rmopd-15
    Request PDUs: 0, Response PDUs: 0,
    Request Variables: 0, Response Variables: 0,
    Average Response Time(ms): 0.00,
    Maximum Response Time(ms): 0.00

  Subagent: /var/run/chassisd-30
    Request PDUs: 33116, Response PDUs: 33116,
    Request Variables: 33116, Response Variables: 33116,
    Average Response Time(ms): 1.83,
    Maximum Response Time(ms): 203.48

  Subagent: /var/run/pkid-13
    Request PDUs: 0, Response PDUs: 0,
    Request Variables: 0, Response Variables: 0,
    Average Response Time(ms): 0.00,
```

```
  Maximum Response Time(ms): 0.00

Subagent: /var/run/apsd-13
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/dfcd-32
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/mib2d-33
  Request PDUs: 74211, Response PDUs: 74211,
  Request Variables: 74211, Response Variables: 74211,
  Average Response Time(ms): 2.30,
  Maximum Response Time(ms): 51.04

Subagent: /var/run/license-check-16
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/craftd-14
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/bfdd-19
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/smihelperd-24
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/cfmd-18
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/rpd_snmp
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/l2tpd-18
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00
```


Copyright © 2018, Juniper Networks, Inc.

show snmp v3

Syntax

show snmp v3
<access <brief | detail> | community | general | groups | notify <filter> | target <address | parameters> | users>

Release Information

Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Display the Simple Network Management Protocol version 3 (SNMPv3) operating configuration.

Options

none—Display all of the SNMPv3 operating configuration.

access—(Optional) Display SNMPv3 access information.

brief | detail—(Optional) Display brief or detailed information about SNMPv3 access information.

community—(Optional) Display SNMPv3 community information.

general—(Optional) Display SNMPv3 general information.

groups—(Optional) Display SNMPv3 security-to-group information.

notify <filter>—(Optional) Display SNMPv3 notify information and, optionally, notify filter information.

target <address | parameters>—(Optional) Display SNMPv3 target information and, optionally, either target address or target parameter information.

users—(Optional) Display SNMPv3 user information.

Additional Information

To edit the default display of the **show snmp v3** command, specify options in the **show** statement at the **[edit snmp v3]** hierarchy level.

Required Privilege Level

view

Related Documentation

- SNMPv3 Overview on page 215
- Minimum SNMPv3 Configuration on a Device Running Junos OS on page 216
- Configuring Access Privileges for a Group on page 267

List of Sample Output

show snmp v3 on page 421

Output Fields

Table 55 on page 421 describes the output fields for the **show snmp v3** command. Output fields are listed in the approximate order in which they appear.

Copyright © 2018, Juniper Networks, Inc.

Table 55: show snmp v3 Output Fields

Field Name	Field Description
Local engine	Information about the local SNMP engine configuration: • **Local engine ID**—Unique Identifier of the local SNMPv3 engine. • **Engine boots**—Number of times the local SNMPv3 engine has rebooted or reinitialized since this engine ID was configured. • **Engine time**—Number of seconds since the local SNMPv3 engine was last rebooted or reinitialized. • **Max msg size**—Maximum message size the sender can accommodate.
Engine ID (local engine)	Information about the local SNMP engine ID and the associated users: • **User**—SNMPv3 username. • **Auth/Priv**—Authentication and encryption algorithm that is configured for the user. • **Storage**—Indicates whether a username is saved to the configuration file (nonvolatile) or not saved (volatile). Applies only to users with active status. • **Status**—Status of the user as listed in the SNMPv3 user table. Only rows with an active status in the table are used by the SNMPv3 engine.
Engine ID (remote engine)	Information about a remote SNMP engine, associated users, user groups, and user access policies: • **User**—SNMPv3 username. • **Auth/Priv**—Authentication and encryption algorithm that is configured for the user. • **Storage**—Indicates whether a username is saved to the configuration file (nonvolatile) or not (volatile). Applies only to users with active status. • **Status**—Status of a new user that has been activated. Only users with an active status can use SNMPv3. • **Group name**—Name of a group of users for which the configured access privileges apply. • **Security model**—Security model (such as **usm**, **v1**, **v2c**, or **any**) that is configured for the group. The security model is used with the security name to ensure messaging security. • **Security name**—Security name that is associated with a user, and which is used with the security model to ensure messaging security. • **Storage type**—Indicates whether a username is saved to the configuration file (nonvolatile) or not saved (volatile). Applies only to users with active status. • **Status**—Status of a user in a group. Only users with an active status can use SNMPv3.
Access control	Information about access control: • **Group name**—Name of a group of users for which the configured access privileges apply. • **Context prefix**—SNMPv3 context for which the configured access privileges apply. • **Security model/level**—Security model and security level combination that is configured for user access privileges. • **Read view**—Identifies the MIB view used for SNMPv3 read operations. • **Write view**—Identifies the MIB view used for SNMPv3 write operations. • **Notify view**—Identifies the MIB view used for outbound SNMP notifications.

Sample Output

show snmp v3

```
user@host> show snmp v3
```

```
Local engine ID: 80 00 0a 4c e04 31 32 33 34
Engine boots:          38
Engine time:        64583 seconds
Max msg size:        2048 bytes

Engine ID: local
    User                            Auth/Priv   Storage      Status
    user1                            md5/des    nonvolatile  active
    user2                            sha/none   nonvolatile  active
    user3                           none/none   nonvolatile  active

Engine ID: 81 00 0a 4c 04 64 64 64 64
    User                            Auth/Priv   Storage      Status
    UNEW                             md5/none   nonvolatile  active
Group name           Security  Security              Storage      Status
                     model     name                  type
g1                   usm       user1                 nonvolatile  active
g2                   usm       user2                 nonvolatile  active
g3                   usm       user3                 nonvolatile  active

Access control:
Group                Context Security      Read       Write     Notify
                     prefix  model/level   view       view      view
g1                            usm/privacy  v1         v1
g2                            usm/authent  v1         v1
g3                            usm/none     v1         v1
```


Copyright © 2018, Juniper Networks, Inc.

PART 6

System Logging

- Configuring System Logging on page 425
- System Logging Configuration Statements on page 461
- System Logging Operational Commands on page 481

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 16

Configuring System Logging

- Overview of Junos OS System Log Messages on page 426
- Overview of Single-Chassis System Logging Configuration on page 426
- Junos OS Minimum System Logging Configuration on page 428
- Junos OS System Log Configuration Statements on page 428
- Adding a Text String to System Log Messages Directed to a Remote Destination on page 429
- Directing System Log Messages to a Log File on page 430
- Directing System Log Messages to a Remote Machine on page 431
- Directing System Log Messages to a User Terminal on page 431
- Directing System Log Messages to the Console on page 432
- Disabling the System Logging of a Facility on page 432
- Displaying a Log File from a Single-Chassis System on page 433
- Including Priority Information in System Log Messages on page 434
- Including the Year or Millisecond in Timestamps on page 435
- Logging Messages in Structured-Data Format on page 436
- Interpreting Messages Generated in Structured-Data Format on page 437
- Interpreting Messages Generated in Standard Format on page 440
- Specifying Log File Size, Number, and Archiving Properties on page 441
- Specifying the Facility and Severity of Messages to Include in the Log on page 442
- Junos OS System Logging Facilities and Message Severity Levels on page 444
- Default Facilities for System Log Messages Directed to a Remote Destination on page 446
- Alternate Facilities for System Log Messages Directed to a Remote Destination on page 446
- Changing the Alternative Facility Name for System Log Messages Directed to a Remote Destination on page 447
- Using Regular Expressions to Refine the Set of Logged Messages on page 449
- Displaying a Log File from a Single-Chassis System on page 451
- Monitoring System Log Messages on page 453
- Examples: Configuring System Logging on page 454

Copyright © 2018, Juniper Networks, Inc.

- Examples: Assigning an Alternative Facility on page 456
- Example: Configuring System Log Messages on page 457

Overview of Junos OS System Log Messages

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

- Routine operations, such as a user login into the configuration database.
- Failure and error conditions, such as failure to access a configuration file.
- Emergency or critical conditions, such as power-down of the switch 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 System Log Explorer.

NOTE: OCX Series switches comprise both the Junos OS and the host operating system (OS). For information about system logging on the host OS, see *Managing Host OS System Log and Core Files*.

Related Documentation

- Junos OS System Log Configuration Statements on page 428
- Junos OS Minimum System Logging Configuration on page 428

Overview of Single-Chassis System Logging Configuration

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

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 442.

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 430.
- To the terminal session of one or more specific users (or all users) when they are logged in to the switch, by including the **user** statement. See "Directing System Log Messages to a User Terminal" on page 431.

Copyright © 2018, Juniper Networks, Inc.

- To the switch console, by including the **console** statement. See "Directing System Log Messages to the Console" on page 432.
- To a remote machine that is running the **syslogd** utility, by including the **host** statement. See "Directing System Log Messages to a Remote Machine" on page 431.

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 *Junos OS System Log Messages Reference*. 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 OS 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 436.
- A message's facility and severity level are together referred to as its *priority*. By default, the standard Junos OS 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 434.
- By default, the standard Junos OS 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 435.
- 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 Junos OS or messages generated on particular switches. For more information, see "Directing System Log Messages to a Remote Machine" on page 431.
- 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 449.

NOTE: During a commit check, warnings about the **traceoptions** configuration (for example, mismatch in trace file sizes or number of trace files) are not displayed on the console. However, these warnings are logged in the system log messages when the new configuration is committed.

Related Documentation

- Examples: Configuring System Logging on page 454
- Specifying the Facility and Severity of Messages to Include in the Log on page 442
- Junos OS System Logging Facilities and Message Severity Levels on page 444

- Directing System Log Messages to a Log File on page 430
- Directing System Log Messages to a Remote Machine on page 431
- Directing System Log Messages to a User Terminal on page 431
- Directing System Log Messages to the Console on page 432

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 56 on page 428. For more information about the configuration statements, see *Single-Chassis System Logging Configuration Overview*.

Table 56: 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;
	}

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*

Junos OS System Log Configuration Statements

To configure the switch 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 {
```


Copyright © 2018, Juniper Networks, Inc.

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

Related Documentation

- Overview of Junos OS System Log Messages on page 426

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*
- Specifying Log File Size, Number, and Archiving Properties on page 441

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 442.

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 441.

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

- **explicit-priority**—See "Including Priority Information in System Log Messages" on page 434
- **match**—See "Using Regular Expressions to Refine the Set of Logged Messages" on page 449
- **structured-data**—See *Logging Messages in Structured-Data Format*

Related Documentation

- *Single-Chassis System Logging Configuration Overview*
- Overview of Junos OS System Log Messages on page 426
- *Logging Messages in Structured-Data Format*
- *Examples: Configuring System Logging*

Copyright © 2018, Juniper Networks, Inc.

Directing System Log Messages to a Remote Machine

To direct system log messages to a remote machine, 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;
```

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 or fully qualified hostname. The remote machine must be running the standard **syslogd** utility. We do not recommend directing messages to another Juniper Networks switch. 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.

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" on page 442.

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 434.

For information about the **match** statement, see "Using Regular Expressions to Refine the Set of Logged Messages" on page 449.

When directing messages to remote machines, you can include the **source-address** statement to specify the IP address of the switch that is reported in the messages as their source. In each **host** statement, you can also include the **facility-override** statement to assign an alternative facility and the **log-prefix** statement to add a string to each message.

Related Documentation

- Overview of Single-Chassis System Logging Configuration on page 426

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 442. For information about the **match** statement, see "Using Regular Expressions to Refine the Set of Logged Messages" on page 449.

Related Documentation

- *Single-Chassis System Logging Configuration Overview*
- *Examples: Configuring System Logging*

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 442.

Related Documentation

- *Single-Chassis System Logging Configuration Overview*
- *Examples: Configuring System Logging*

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;
}
```


Copyright © 2018, Juniper Networks, Inc.

Related Documentation

- *Single-Chassis System Logging Configuration Overview*

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 the following commands:

user@switch> **show log** *log-filename*
user@switch> **file show** *log-file-pathname*

By default, the commands display the file stored on the local Routing Engine.

The following example shows the output from the **show log messages** command:

```
user@switch1> show log messages
Nov  4 11:30:01 switch1 newsyslog[2283]: logfile turned over due to size>128K
Nov  4 11:30:01 switch1 newsyslog[2283]: logfile turned over due to size>128K
Nov  4 11:30:06  switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent
 for Fan 1
Nov  4 11:30:06  switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent
 for Fan 2
Nov  4 11:30:06  switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent
 for Fan 3
...
Nov  4 11:52:53  switch1 snmpd[944]: SNMPD_HEALTH_MON_INSTANCE: Health Monitor:
jroute daemon memory usage (Management
process): new instance detected (variable: sysApplElmtRunMemory.5.6.2293)
Nov  4 11:52:53  switch1 snmpd[944]: SNMPD_HEALTH_MON_INSTANCE: Health Monitor:
jroute daemon memory usage (Command-line
interface): new instance detected (variable: sysApplElmtRunMemory.5.8.2292)
...
Nov  4 12:08:30  switch1 rpdf[957]: task_connect: task BGP_100.10.10.1.6+179 addr
 10.10.1.6+179: Can't assign requested
address
Nov  4 12:08:30  switch1 rpdf[957]: bgp_connect_start: connect 10.10.1.6 (Internal
 AS 100): Can't assign requested address
Nov  4 12:10:24  switch1 mgd[2293]: UI_CMDLINE_READ_LINE: User 'jsmith', command
 'exit '
Nov  4 12:10:27  switch1 mgd[2293]: UI_DBASE_LOGOUT_EVENT: User 'jsmith' exiting
 configuration mode
Nov  4 12:10:31  switch1 mgd[2293]: UI_CMDLINE_READ_LINE: User 'jsmith', command
 'show log messages
```

The following example shows the output from the **file show** command. The file in the pathname **/var/log/processes** has been previously configured to include messages from the daemon facility.

```
user@switch1> file show /var/log/processes
Feb 22 08:58:24 switch1 snmpd[359]: SNMPD_TRAP_WARM_START: trap_generate_warm:
SNMP trap: warm start
Feb 22 20:35:07 switch1 snmpd[359]: SNMPD_THROTTLE_QUEUE_DRAINED:
trap_throttle_timer_handler: cleared all throttled traps
Feb 23 07:34:56 switch1 snmpd[359]: SNMPD_TRAP_WARM_START: trap_generate_warm:
SNMP trap: warm start
Feb 23 07:38:19 switch1 snmpd[359]: SNMPD_TRAP_COLD_START: trap_generate_cold:
```

```
SNMP trap: cold start
...
```

Related Documentation

- Interpreting Messages Generated in Standard Format on page 440
- Interpreting Messages Generated in Structured-Data Format on page 437

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*. 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 447.

Copyright © 2018, Juniper Networks, Inc.

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*
- *Examples: Configuring System Logging*

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 15:36:30
```

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);
```

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.

The following example illustrates the format for a timestamp that includes both the millisecond (401) and the year (2010):

```
Aug 21 15:36:30.401 2010
```

NOTE: By default, messages logged in structured-data format include the year and millisecond. 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 436. For information about interpreting messages in a structured-data format, see "Interpreting Messages Generated in Structured-Data Format" on page 437.

Logging Messages in Structured-Data Format

You can log messages to a file in structured-data format instead of the standard Junos OS format. The 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-21.txt**. 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. For information about the fields in a structured-data–format message, see "Interpreting Messages Generated in Structured-Data Format" on page 437.

The structured format is used for all messages logged to the file that are generated by a Junos OS 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.

Copyright © 2018, Juniper Networks, Inc.

Interpreting Messages Generated in Structured-Data Format

By default, Junos OS processes and software libraries write messages to the system log file in structured-data format. For information about the **structured-data** statement, see *Logging Messages in Structured-Data Format*.

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.

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 57 on page 437 describes the fields. If the system logging utility cannot determine the value in a particular field, a hyphen (-) appears instead.

Table 57: Fields in Structured-Data Messages

Field	Description	Examples
<priority code>	Number that indicates the facility and severity of a message. 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 "Specifying the Facility and Severity of Messages to Include in the Log" on page 442.	<165> for a message from the **pfe** facility (facility=20) with severity **notice** (severity=5).
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.	switch1

Table 57: Fields in Structured-Data Messages *(continued)*

Field	Description	Examples
process	Name of the Junos OS process that generated the message.	mgd
processID	UNIX process ID (PID) of the Junos 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 the Junos OS. It is followed by a dot-separated numerical identifier for the platform type.	junos@2636.1.1.1.2.18
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).	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 58 on page 439 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 58 on page 439 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 442.

Copyright © 2018, Juniper Networks, Inc.

Table 58: Facility and Severity Codes in the priority-code Field

Facility (number)	Severity 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
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

Copyright © 2018, Juniper Networks, Inc.

Interpreting Messages Generated in Standard Format

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***] 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 59 on page 440 describes the message fields.

Table 59: Fields in Standard-Format Messages

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: hostname, process and process ID (PID). If the process does not report its PID, the PID is not displayed. The message source subfields are displayed in the following format: *hostname process[process-ID]*
facility	Code that specifies the facility to which the system log message belongs. For a mapping of codes to facility names, see Table: **Facility Codes Reported in Priority Information** in "Including Priority Information in System Log Messages" on page 434.
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 434.
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.

Copyright © 2018, Juniper Networks, Inc.

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*
- *Examples: Configuring System Logging*
- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

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 ;
}
```


Copyright © 2018, Juniper Networks, Inc.

For more information about the destinations, see "Directing System Log Messages to a User Terminal" on page 431, and, "Directing System Log Messages to the Console" on page 432.

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 60 on page 443 lists the Junos OS system logging facilities that you can specify in configuration statements at the **[edit system syslog]** hierarchy level.

Table 60: 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
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 61 on page 444 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 432.

Copyright © 2018, Juniper Networks, Inc.

Table 61: 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
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 444
- *Single-Chassis System Logging Configuration Overview*
- *Examples: Configuring System Logging*

Junos OS System Logging Facilities and Message Severity Levels

Table 60 on page 443 lists the Junos OS system logging facilities that you can specify in configuration statements at the **[edit system syslog]** hierarchy level.

Table 62: 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

Copyright © 2018, Juniper Networks, Inc.

Table 62: Junos OS System Logging Facilities *(continued)*

Facility	Type of Event or Error
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 61 on page 444 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 432.

Table 63: 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

Copyright © 2018, Juniper Networks, Inc.

Table 63: 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

- *Single-Chassis System Logging Configuration Overview*
- *Examples: Configuring System Logging*

Default Facilities for System Log Messages Directed to a Remote Destination

Table 64 on page 446 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 64: 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
interactive-commands	local7
pfe	local4

Related Documentation

- *Single-Chassis System Logging Configuration Overview*

Alternate Facilities for System Log Messages Directed to a Remote Destination

Table 65 on page 446 lists the facilities that you can specify in the **facility-override** statement.

Table 65: Facilities for the facility-override Statement

Facility	Description
authorization	Authentication and authorization attempts

Copyright © 2018, Juniper Networks, Inc.

Table 65: Facilities for the facility-override Statement *(continued)*

Facility	Description
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*
- *Single-Chassis System Logging Configuration Overview*

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 "Junos OS System Logging Facilities and Message Severity Levels" on page 443). 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 64 on page 446 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 65 on page 446 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;
```

 Copyright © 2018, Juniper Networks, Inc.

```
}
```

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 64 on page 446
- Alternate Facilities for System Log Messages Directed to a Remote Destination on page 446
- *Examples: Assigning an Alternative Facility to System Log Messages Directed to a Remote Destination*

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 66 on page 450 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 66: 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.
^ (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.

Copyright © 2018, Juniper Networks, Inc.

Table 66: Regular Expression Operators for the match Statement *(continued)*

Operator	Matches
( ) (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*
- *Examples: Configuring System Logging*

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 the following commands:

user@switch> **show log** *log-filename*

user@switch> **file show** *log-file-pathname*

By default, the commands display the file stored on the local Routing Engine.

The following example shows the output from the **show log messages** command:

```
user@switch1> show log messages
Nov  4 11:30:01 switch1 newsyslog[2283]: logfile turned over due to size>128K
Nov  4 11:30:01 switch1 newsyslog[2283]: logfile turned over due to size>128K
Nov  4 11:30:06  switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent
 for Fan 1
Nov  4 11:30:06  switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent
 for Fan 2
Nov  4 11:30:06  switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent
 for Fan 3
...
Nov  4 11:52:53  switch1 snmpd[944]: SNMPD_HEALTH_MON_INSTANCE: Health Monitor:
jroute daemon memory usage (Management
process): new instance detected (variable: sysApplElmtRunMemory.5.6.2293)
Nov  4 11:52:53  switch1 snmpd[944]: SNMPD_HEALTH_MON_INSTANCE: Health Monitor:
jroute daemon memory usage (Command-line
interface): new instance detected (variable: sysApplElmtRunMemory.5.8.2292)
...
Nov  4 12:08:30  switch1 rpdf[957]: task_connect: task BGP_100.10.10.1.6+179 addr
 10.10.1.6+179: Can't assign requested
address
Nov  4 12:08:30  switch1 rpdf[957]: bgp_connect_start: connect 10.10.1.6 (Internal
 AS 100): Can't assign requested address
Nov  4 12:10:24  switch1 mgd[2293]: UI_CMDLINE_READ_LINE: User 'jsmith', command
 'exit '
Nov  4 12:10:27  switch1 mgd[2293]: UI_DBASE_LOGOUT_EVENT: User 'jsmith' exiting
 configuration mode
Nov  4 12:10:31  switch1 mgd[2293]: UI_CMDLINE_READ_LINE: User 'jsmith', command
 'show log messages
```

The following example shows the output from the **file show** command. The file in the pathname **/var/log/processes** has been previously configured to include messages from the daemon facility.

```
user@switch1> file show /var/log/processes
Feb 22 08:58:24 switch1 snmpd[359]: SNMPD_TRAP_WARM_START: trap_generate_warm:
SNMP trap: warm start
Feb 22 20:35:07 switch1 snmpd[359]: SNMPD_THROTTLE_QUEUE_DRAINED:
trap_throttle_timer_handler: cleared all throttled traps
Feb 23 07:34:56 switch1 snmpd[359]: SNMPD_TRAP_WARM_START: trap_generate_warm:
SNMP trap: warm start
Feb 23 07:38:19 switch1 snmpd[359]: SNMPD_TRAP_COLD_START: trap_generate_cold:
SNMP trap: cold start
...
```

Related Documentation

- Interpreting Messages Generated in Standard Format on page 440
- Interpreting Messages Generated in Structured-Data Format on page 437

Copyright © 2018, Juniper Networks, Inc.

Monitoring System Log Messages

Purpose Display system log messages about the QFX Series. By looking through a system log file for any entries pertaining to the interface that you are interested in, you can further investigate a problem with an interface on the switch.

Action To view system log messages:

user@switch1> **show log messages**

Sample Output

```
Nov  4 11:30:01 switch1 newsyslog[2283]: logfile turned over due to size>128K
Nov  4 11:30:01 switch1 newsyslog[2283]: logfile turned over due to size>128K
Nov  4 11:30:06  switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent
 for Fan 1
Nov  4 11:30:06  switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent
 for Fan 2
Nov  4 11:30:06  switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent
 for Fan 3
...
Nov  4 11:52:53  switch1 snmpd[944]: SNMPD_HEALTH_MON_INSTANCE: Health Monitor:
jroute daemon
memory usage (Management process): new instance detected (variable:
sysApplElmtRunMemory.5.6.2293)
Nov  4 11:52:53  switch1 snmpd[944]: SNMPD_HEALTH_MON_INSTANCE: Health Monitor:
jroute daemon
memory usage (Command-line interface): new instance detected (variable:
sysApplElmtRunMemory.5.8.2292)
...
Nov  4 12:10:24  switch1 mgd[2293]: UI_CMDLINE_READ_LINE: User 'jsmith', command
 'exit '
Nov  4 12:10:27  switch1 mgd[2293]: UI_DBASE_LOGOUT_EVENT: User 'jsmith' exiting
 configuration mode
Nov  4 12:10:31  switch1 mgd[2293]: UI_CMDLINE_READ_LINE: User 'jsmith', command
 'show log messages
```

Meaning The sample output shows the following entries in the **messages** file:

- A new log file was created when the previous file reached the maximum size of 128 kilobytes (KB).
- The fan speed for Fan 1, 2, and 3 is set at 65 percent.
- Health monitoring activity is detected.
- CLI commands were entered by the user jsmith.

Related Documentation

- Overview of Junos OS System Log Messages on page 426
- *Understanding the Implementation of System Log Messages on the QFabric System*
- Example: Configuring System Log Messages on page 457

- *clear log*
- show log on page 482
- syslog on page 477

Examples: Configuring System Logging

The system log provides an excellent way of tracking all management activity on the switch by recording events such as user authentication, access authorization, and command execution. Logged command executions include commands entered by users at the CLI prompt or by client applications such as the Junos XML protocol or NETCONF XML client. Because system log files contain information about commands executed on the switch and the user who executed the commands, checking system log files for failed authentication events can help identify attempts to hack in to the switch. You can also analyze network activity by correlating executed commands with events and changes that occurred on the network at a particular time.

System log files are stored locally on the switch in the default **/var/log** directory.

The following example shows how to configure system log messages to record all commands entered by users and all authentication or authorization attempts. Logged commands include those entered by users at the CLI prompt and by client applications. Authentication and authorization attempts include events that are saved in the file named **cli-commands** and those that are sent to the terminal of a 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 log all alarms state changes 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 {
```

 Copyright © 2018, Juniper Networks, Inc.

```
    /* 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 info, notice, and warning severity levels:

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

The following list describes the security levels used in the example:

- **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 command **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.

Related Documentation

- Overview of Single-Chassis System Logging Configuration on page 426

Examples: Assigning an Alternative Facility

This topic contains examples of configuring system log messages to use an alternative facility for logging.

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

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

The following example contains two sets of statements that show how to configure switches located in California and in New York to send messages to a single remote host 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**.

- The following statements configure the California switch to aggregate messages in the **local0** facility:

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

- The following statements configure the New York switch to aggregate messages in the **local2** facility:

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

On the remote host named **central-logger** you can subsequently configure the system logging utility to write messages from the **local0** facility to one file (for example, **california-config**) and the messages from the **local2** facility to another file (for example, **new-york-config**).

Related Documentation

- Alternate Facilities for System Log Messages Directed to a Remote Destination on page 446

Copyright © 2018, Juniper Networks, Inc.

Example: Configuring System Log Messages

The QFabric system monitors events that occur on its component devices and distributes system log messages about those events to all external system log message servers (hosts) that are configured. Component devices may include Node devices, Interconnect devices, Director devices, and the Virtual Chassis. Messages are stored for viewing only in the QFabric system database. To view the messages, issue the **show log** command.

This example describes how to configure system log messages on the QFabric system.

- Requirements on page 457
- Overview on page 457
- Configuration on page 457

Requirements

This example uses the following hardware and software components:

- Junos OS Release 12.2
- QFabric system
- External servers that can be configured as system log message hosts

Overview

Component devices that generate system log message events may include Node devices, Interconnect devices, Director devices, and the control plane switches. The following configuration example includes these components in the QFabric system:

- Director software running on the Director group
- Control plane switches
- Interconnect device
- Multiple Node devices

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set system syslog host 10.1.1.12 any error
set system syslog file qflogs
set system syslog file qflogs structured-data brief
set system syslog file qflogs archive size 1g
```

Step-by-Step Procedure

The following example requires that you navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure system messages from the QFabric Director device:

1. Specify a host, any facility, and the **error** severity level.

```
[edit system syslog]
user@switch# set host 10.1.1.12 any error
```

NOTE: You can configure more than one system log message server (host). The QFabric system sends the messages to each server configured.

2. (Optional) Specify a filename to capture log messages.

NOTE: On the QFabric system, a syslog file named **messages** is configured implicitly with facility and severity levels of **any any** and a file size of 100 MBs. Therefore, you cannot specify the filename **messages** in your configuration, and automatic command completion does not work for that filename.

```
[edit system syslog]
user@switch# set file qflogs structured-data brief
user@switch# set file qflogs
```

3. (Optional) Configure the maximum size of your system log message archive file. This example specifies an archive size of 1 GB.

```
[edit system syslog]
user@switch# set file qflogs archive size 1g
```

Results

From configuration mode, confirm your configuration by entering the **show system** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@switch# show system
syslog {
   file qflogs {
   }
   host 10.1.1.12 {
      any error;
   }
}
```


Copyright © 2018, Juniper Networks, Inc.

If you are done configuring the device, enter **commit** from configuration mode.

Related Documentation

- *Understanding the Implementation of System Log Messages on the QFabric System*
- *syslog (QFabric System)*
- show log on page 482

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 17

System Logging Configuration Statements

- archive (All System Log Files) on page 462
- archive (Individual System Log File) on page 464
- console (System Logging) on page 466
- explicit-priority on page 467
- facility-override on page 468
- file (System Logging) on page 469
- files on page 470
- host (System) on page 471
- log-prefix (System) on page 473
- match on page 474
- size (System) on page 475
- structured-data on page 476
- syslog (System) on page 477
- time-format on page 479
- user (System Logging) on page 480

Copyright © 2018, Juniper Networks, Inc.

archive (All System Log Files)

Syntax

```
archive <files number> <size size> <start-time time> <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**

Copyright © 2018, Juniper Networks, Inc.

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 441

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

Copyright © 2018, Juniper Networks, Inc.

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 441

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 "Junos OS System Logging Facilities and Message Severity Levels" on page 443.

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 432
- System Log Explorer

Copyright © 2018, Juniper Networks, Inc.

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 434
- System Log Explorer
- **structured-data on page 476**

facility-override

Syntax facility-override *facility*;

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 Substitute an alternate facility for the default facilities used when messages are directed to a remote destination.

Options ***facility***—Alternate facility to substitute for the default facilities. For a list of the possible facilities, see Table 65 on page 446.

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

Related Documentation
- Changing the Alternative Facility Name for System Log Messages Directed to a Remote Destination on page 447
- System Log Explorer

 Copyright © 2018, Juniper Networks, Inc.

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 "Junos OS System Logging Facilities and Message Severity Levels" on page 443.

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 "Junos OS System Logging Facilities and Message Severity Levels" on page 444.

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 430
- *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 475

 Copyright © 2018, Juniper Networks, Inc.

host (System)

Syntax

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

QFX Series and OCX Series

```
host (hostname {
   facility severity;
   explicit-priority;
   facility-override facility;
   log-prefix string;
   match "regular-expression";
   match-string string-name;
   port;
   source-address source-address;
}
```

TX Matrix Router and EX Series Switches

```
host (hostname | other-routing-engine | scc-master) {
   facility severity;
   explicit-priority;
   facility-override facility;
   log-prefix string;
   match "regular-expression";
   match-string string-name;
   port;
   source-address source-address;
}
```

TX Matrix Plus Router

```
host (hostname | other-routing-engine | sfc0-master) {
   facility severity;
   allow-duplicates;
   explicit-priority;
   facility-override facility;
   log-prefix (System) string;
   match "regular-expression";
   match-string string-name;
   port;
   source-address source-address;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* system syslog],
[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 a remote destination.

Options

facility—Class of messages to log. To specify multiple classes, include multiple ***facility severity*** statements. For a list of the facilities, see "Junos OS System Logging Facilities and Message Severity Levels" on page 443.

hostname—IPv4 address, IPv6 address, or fully qualified hostname of the remote machine to which to direct messages. To direct messages to multiple remote machines, include a **host** statement for each one.

other-routing-engine—Direct messages to the other Routing Engine on a router or switch with two Routing Engines installed and operational.

NOTE: **The other-routing-engine option is not applicable to the QFX Series and OCX Series.**

port—Port number of the remote syslog server that can be modified.

scc-master—(TX Matrix routers only) On a T640 router that is part of a routing matrix, direct messages to the TX Matrix router.

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 "Junos OS System Logging Facilities and Message Severity Levels" on page 444.

sfc0-master—(TX Matrix Plus routers only) On a T1600 or T4000 router that is part of a routing matrix, direct messages to the TX Matrix Plus router.

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 Remote Machine or the Other Routing Engine*
- *Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router*
- *Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router*
- *Junos OS System Log Reference*

Copyright © 2018, Juniper Networks, Inc.

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 429
- *Junos OS System Log Reference for Security Devices*

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 449
- *match-string*

Copyright © 2018, Juniper Networks, Inc.

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 441
- System Log Explorer
- files on page 470

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*
- *Junos OS System Log Reference for Security Devices*
- explicit-priority on page 467
- time-format on page 479

Copyright © 2018, Juniper Networks, Inc.

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*
- System Log Explorer

Copyright © 2018, Juniper Networks, Inc.

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**.

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
```

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*
- *Junos OS System Log Reference for Security Devices*
- structured-data on page 476

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 "Junos OS System Logging Facilities and Message Severity Levels" on page 443.

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 "Junos OS System Logging Facilities and Message Severity Levels" on page 444.

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 431
- Junos OS System Logging Facilities and Message Severity Levels on page 444
- *Junos OS System Log Reference for Security Devices*

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 18

System Logging Operational Commands

- show log

show log

List of Syntax

Syntax on page 482
Syntax (QFX Series and OCX Series) on page 482
Syntax (TX Matrix Router) on page 482

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).

Copyright © 2018, Juniper Networks, Inc.

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 477

List of Sample Output

show log on page 484
show log filename on page 484
show log filename (QFabric System) on page 484
show log user on page 485

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,
```


Copyright © 2018, Juniper Networks, Inc.

```
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)
```

Copyright © 2018, Juniper Networks, Inc.