



SRC PE Software

Monitoring and Troubleshooting Guide

Release

4.12.x



Modified: 2018-10-15

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

Copyright © 2018 Juniper Networks, Inc. All rights reserved.

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.

SRC PE Software Monitoring and Troubleshooting Guide
Release 4.12.x
Copyright © 2018 Juniper Networks, Inc. All rights reserved.

Revision History
October 2018—Revision 1

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.

SOFTWARE LICENSE

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

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

Abbreviated Table of Contents

	About the Documentation	xvii
Part 1	Monitoring and Troubleshooting the SRC Software and C Series Controllers	
Chapter 1	Overview of Monitoring and Troubleshooting Tools	3
Part 2	Using Logging for the SRC Software and C Series Controllers	
Chapter 2	Configuring Logging for SRC Components	7
Chapter 3	Configuring Logging for SRC Components with the CLI	25
Chapter 4	Configuring Logging for SRC Components (C-Web Interface)	39
Part 3	Using Simulated Router Drivers and Simulated Subscribers for Testing	
Chapter 5	Configuring a Simulated Router Driver for Testing (SRC CLI)	45
Chapter 6	Configuring a Simulated Router Driver for Testing (C-Web Interface)	49
Chapter 7	Using Simulated Subscribers for Testing (SRC CLI)	51
Part 4	Using SNMP for Monitoring and Troubleshooting	
Chapter 8	Creating Custom SNMP Monitors	61
Chapter 9	Configuring SNMP Chassis Alarms	73
Chapter 10	Configuring the SNMP Traps (SRC CLI)	83
Chapter 11	Understanding Traps	89
Part 5	Monitoring the SRC Software and the C Series Controller with the C-Web Interface and the SRC CLI	
Chapter 12	Monitoring with the SRC CLI and the C-Web Interface	111
Chapter 13	Monitoring the System (SRC CLI)	115
Chapter 14	Monitoring the System (C-Web Interface)	123
Chapter 15	Monitoring SAE Data (SRC CLI)	133
Chapter 16	Monitoring SAE Data (C-Web Interface)	169
Chapter 17	Monitoring and Troubleshooting the NIC (SRC CLI)	195
Chapter 18	Monitoring the NIC (C-Web Interface)	207
Chapter 19	Monitoring NTP (SRC CLI)	213
Chapter 20	Monitoring NTP (C-Web Interface)	217

Chapter 21	Monitoring Redirect Server (SRC CLI)	221
Chapter 22	Monitoring the Redirect Server and Filtered Traffic (C-Web Interface) . .	223
Chapter 23	Troubleshooting Network Connectivity (SRC CLI)	227
Chapter 24	Monitoring Network Connectivity (C-Web Interface)	233
Chapter 25	Monitoring Activity for SRC Components	235

Table of Contents

	About the Documentation	xvii
	SRC Documentation and Release Notes	xvii
	Audience	xvii
	Documentation Conventions	xvii
	Documentation Feedback	xix
	Requesting Technical Support	xx
	Self-Help Online Tools and Resources	xx
	Opening a Case with JTAC	xx
Part 1	Monitoring and Troubleshooting the SRC Software and C Series Controllers	
Chapter 1	Overview of Monitoring and Troubleshooting Tools	3
	Monitoring and Troubleshooting Tools Overview	3
Part 2	Using Logging for the SRC Software and C Series Controllers	
Chapter 2	Configuring Logging for SRC Components	7
	Logging for SRC Components Overview	7
	Categories and Severity Levels for Event Messages	7
	Defining Categories	8
	Defining Severity Levels	18
	Defining Filters	19
	Enabling Network Device-Specific Filtering for SAE Debug and Info Logs (SRC CLI)	20
	Rotating Log Files	22
	Configuration Overview	23
Chapter 3	Configuring Logging for SRC Components with the CLI	25
	Configuration Statements for SRC Component Logging	25
	Configuring an SRC Component to Store Log Messages in a File (SRC CLI)	26
	Configuring System Logging (SRC CLI)	28
	Configuration Statements for the Logrotate Utility (SRC CLI)	30
	Configuring the Logrotate Utility (SRC CLI)	32
	Configuring the Global Options for the Logrotate Utility	35
	Configuring Log Rotation Options for Specific Logging Configuration Files	36
	Configuring Logging Rotation Options for System and SRC Components (SRC CLI)	36

Chapter 4	Configuring Logging for SRC Components (C-Web Interface)	39
	Before You Configure Logging for SRC Components	39
	Configuring ACP to Store Log Messages in a File (C-Web Interface)	39
	Configuring the SAE to Store Log Messages in a File (C-Web Interface)	40
	Configuring NIC to Store Log Messages in a File (C-Web Interface)	40
	Configuring the SNMP to Store Log Messages in a File (C-Web Interface)	41
Part 3	Using Simulated Router Drivers and Simulated Subscribers for Testing	
Chapter 5	Configuring a Simulated Router Driver for Testing (SRC CLI)	45
	Simulated Router Drivers for the SRC Software Overview	45
	Configuring Simulated Router Drivers (SRC CLI)	45
Chapter 6	Configuring a Simulated Router Driver for Testing (C-Web Interface)	49
	Configuring a Simulated Router Driver for Testing (C-Web Interface)	49
Chapter 7	Using Simulated Subscribers for Testing (SRC CLI)	51
	Simulated Subscribers Overview	51
	Commands to Manage Simulated Subscribers	51
	Logging In Simulated Subscribers (SRC CLI)	52
	Logging In Authenticated DHCP Subscribers	52
	Logging In Authenticated Interface Subscribers	53
	Logging In Unauthenticated DHCP Subscribers	54
	Logging In Unauthenticated Interface Subscribers	54
	Viewing Subscriber Sessions (SRC CLI)	55
	Logging Out Simulated Subscribers (SRC CLI)	56
	Logging Out Subscribers by DN	56
	Logging Out Subscribers by IP Address	56
	Logging Out Subscribers by Login Name	57
	Logging Out Subscribers by Session ID	57
Part 4	Using SNMP for Monitoring and Troubleshooting	
Chapter 8	Creating Custom SNMP Monitors	61
	SNMP Monitoring on C Series Controllers	61
	Configuration Statements for Customized SRC SNMP Monitors	63
	Configuring an SNMP Alarm on a C Series Controller (SRC CLI)	64
	Defining an Alarm for an SNMP Monitor That Compares Object Values (SRC CLI)	65
	Defining an Alarm to Monitor the Status of an Object (SRC CLI)	66
	Defining an Alarm for an SNMP Monitor That Compares Values Against Thresholds (SRC CLI)	67
	Defining a Discontinuity Check to Validate Delta Values (SRC CLI)	68
	Configuring an SNMPv3 Security Name for SNMP Monitoring (SRC CLI)	68
	Defining Events for Which SNMP Sends Notifications (SRC CLI)	69
	Defining Events That Set Values for SNMP MIB Objects (SRC CLI)	69
	Example: SNMP Monitoring of Multiple MIB Objects	70

Chapter 9	Configuring SNMP Chassis Alarms	73
	SNMP Chassis Alarms on a C Series Controller	73
	Configuring SNMP Chassis Alarms (SRC CLI)	74
	Defining Alarm Thresholds for Battery Voltage Sensors	74
	Defining Alarm Thresholds for CPU Sensors	75
	Defining Alarm Thresholds for CPU Core Voltage Sensors	75
	Defining Alarm Thresholds for CPU DIMM Voltage Sensors	76
	Defining Alarm Thresholds for CPU Temperature Sensors	77
	Defining Alarm Thresholds for Fan Speed Sensors	78
	Defining Alarm Thresholds for System Temperature Sensors	78
	Defining Alarm Thresholds for Voltage Sensors	79
Chapter 10	Configuring the SNMP Traps (SRC CLI)	83
	SNMP Traps Overview	83
	MIBs	83
	Configuration MIBs	84
	Traps	84
	SNMP Traps and Informs	85
	Configuration Statements for the SNMP Traps	85
	Configuring Performance Traps (SRC CLI)	86
	Configuring Event Traps (SRC CLI)	87
Chapter 11	Understanding Traps	89
	Performance Traps	89
	R/AV	90
	Trap Numbers in Performance Traps	90
	Decoding Trap Numbers for Raised Trap Actions	91
	Decoding Trap Numbers for Clear Trap Actions	91
	SRC Performance Traps	92
	SAE Performance Traps	92
	Accounting Performance Traps	94
	Authentication Performance Traps	96
	NIC Performance Traps	97
	Router Driver Performance Traps	98
	System Management Performance Traps	100
	Policy Engine Performance Traps	100
	SRC Redirector Performance Traps	101
	SRC ACP Performance Traps	101
	JPS Performance Traps	102
	Chassis Performance Traps	103
	Event Traps	103
	Alarm State Transitions	106
Part 5	Monitoring the SRC Software and the C Series Controller with the C-Web Interface and the SRC CLI	
Chapter 12	Monitoring with the SRC CLI and the C-Web Interface	111
	Monitoring with the SRC CLI and the C-Web Interface	111
	SRC Monitoring Options	111

Chapter 13	Monitoring the System (SRC CLI)	115
	Viewing Information About a C Series Controller (SRC CLI)	115
	Viewing Information About Components Installed (SRC CLI)	117
	Viewing Information About Boot Messages (SRC CLI)	118
	Viewing Information About Security Certificates (SRC CLI)	121
Chapter 14	Monitoring the System (C-Web Interface)	123
	Viewing Information About the System (C-Web Interface)	123
	Viewing the System Date and Time (C-Web Interface)	124
	Viewing Information About Components Installed (C-Web Interface)	125
	Viewing Information About Boot Messages (C-Web Interface)	126
	Viewing Information About Security Certificates (C-Web Interface)	126
	Viewing Information About System Disk Status (C-Web Interface)	127
	Viewing Information About the Users on the System (C-Web Interface)	128
	Viewing Information About the Juniper Networks Database in Community Mode (C-Web Interface)	129
	Viewing Statistics for the Juniper Networks Database (C-Web Interface)	129
	Viewing Information About the SRC CLI (C-Web Interface)	130
	Viewing Information About the SRC CLI (C-Web Interface)	130
	Viewing Information About SRC CLI User Permissions (C-Web Interface)	131
Chapter 15	Monitoring SAE Data (SRC CLI)	133
	Viewing SAE Data with the CLI	133
	Viewing Information About the Directory Blacklist (SRC CLI)	133
	Viewing Information About SAE Device Drivers (SRC CLI)	134
	Viewing the Synchronization Status of SAE Session Stores (SRC CLI)	135
	Viewing Information About SAE Interfaces (SRC CLI)	136
	Viewing Information About SAE Licenses (SRC CLI)	137
	Viewing Information About Policies on the SAE (SRC CLI)	138
	Viewing Login Registrations (SRC CLI)	140
	Viewing Equipment Registrations (SRC CLI)	141
	Viewing Information About Services (SRC CLI)	141
	Viewing Information About Threads (SRC CLI)	144
	Viewing Information About Subscriber Sessions (SRC CLI)	145
	Viewing General Information About Subscriber Sessions (SRC CLI)	146
	Viewing Information About Subscriber Sessions by DN (SRC CLI)	147
	Viewing Information About Subscriber Sessions by IP Address, VPN Identifier, or both (SRC CLI)	148
	Viewing Information About Subscriber Sessions by Login Name (SRC CLI)	150
	Viewing Information About Subscriber Sessions by Service Name (SRC CLI)	151
	Viewing Information About Subscriber Sessions by Session ID (SRC CLI)	152
	Viewing Information About Subscriber Sessions by Accounting User Identifier (SRC CLI)	154
	Viewing the Number of Active Service Sessions (SRC CLI)	155
	Viewing Subscriber Session Count Used by a Managed Router (SRC CLI)	155

	Viewing SAE SNMP Information with the CLI	156
	Viewing Statistics About the Directory (SRC CLI)	156
	Viewing Statistics for Directory Connections (SRC CLI)	157
	Viewing SNMP Information for Client Licenses (SRC CLI)	159
	Viewing SNMP Information for Local Licenses (SRC CLI)	159
	Viewing SNMP Information for Licenses on Virtual Routers (SRC CLI)	160
	Viewing SNMP Information for Policies (SRC CLI)	160
	Viewing SNMP Information for the SAE Server Process (SRC CLI)	161
	Viewing Statistics for RADIUS Clients (SRC CLI)	161
	Viewing SNMP Information for RADIUS Clients (SRC CLI)	162
	Viewing SNMP Information for Routers and Devices (SRC CLI)	163
	Viewing Statistics for Device Drivers (SRC CLI)	163
	Viewing Statistics for Specific Device Drivers (SRC CLI)	164
	Viewing Statistics for Subscriber and Service Sessions (SRC CLI)	166
	Monitoring Statistics for Subscriber and Service Sessions (SRC CLI)	166
Chapter 16	Monitoring SAE Data (C-Web Interface)	169
	Viewing SAE Data (C-Web Interface)	169
	Viewing Information About the Directory Blacklist (C-Web Interface)	169
	Viewing Information About Services (C-Web Interface)	170
	Viewing Information About Licenses (C-Web Interface)	171
	Viewing Information About Policies (C-Web Interface)	172
	Viewing Information About Device Drivers (C-Web Interface)	172
	Viewing Information About Interfaces (C-Web Interface)	174
	Viewing Equipment Registrations (C-Web Interface)	174
	Viewing Login Registrations (C-Web Interface)	176
	Viewing Information About Threads (C-Web Interface)	177
	Viewing Information About Subscriber Sessions (C-Web Interface)	177
	Information about Subscriber Sessions	178
	Viewing Information About Subscriber Sessions by DN (C-Web Interface)	178
	Viewing Information About Subscriber Sessions by IP Address (C-Web Interface)	179
	Viewing Information About Subscriber Sessions by Login Name (C-Web Interface)	180
	Viewing Information About Subscriber Sessions by Service Name (C-Web Interface)	181
	Viewing Information About Subscriber Sessions by Session ID (C-Web Interface)	182
	Viewing SNMP Information (C-Web Interface)	184
	Viewing SNMP Statistics for the Directory (C-Web Interface)	184
	Viewing SNMP Statistics for Directory Connections (C-Web Interface)	185
	Viewing SNMP Statistics for Client Licenses (C-Web Interface)	186
	Viewing SNMP Statistics for Licenses by Device (C-Web Interface)	186
	Viewing SNMP Statistics for Local Licenses (C-Web Interface)	188
	Viewing SNMP Statistics About Policies (C-Web Interface)	188
	Viewing SNMP Statistics About Server Processes (C-Web Interface)	189
	Viewing SNMP Statistics About RADIUS (C-Web Interface)	190
	Viewing SNMP Statistics About RADIUS Clients (C-Web Interface)	191

	Viewing SNMP Statistics for Devices (C-Web Interface)	192
	Viewing SNMP Statistics for Specific Devices (C-Web Interface)	193
	Viewing SNMP Statistics for Subscriber Sessions and Service Sessions (C-Web Interface)	194
Chapter 17	Monitoring and Troubleshooting the NIC (SRC CLI)	195
	SRC CLI Commands to View Statistics About NIC Operations	195
	Viewing Statistics for the NIC Process (SRC CLI)	196
	Viewing Statistics for a NIC Host (SRC CLI)	197
	Viewing Statistics for NIC Resolvers (SRC CLI)	198
	Viewing Statistics for NIC Agents (SRC CLI)	199
	SRC CLI Commands to View NIC Resolution Data	201
	Viewing Data for NIC Resolvers (SRC CLI)	201
	Viewing Data for NIC Agents (SRC CLI)	203
	Troubleshooting NIC Data Resolution (SRC CLI)	205
Chapter 18	Monitoring the NIC (C-Web Interface)	207
	Viewing Hosts (C-Web Interface)	207
	Viewing Host Statistics (C-Web Interface)	207
	Viewing Host Process Statistics (C-Web Interface)	208
	Viewing Resolvers (C-Web Interface)	209
	Viewing Resolvers (C-Web Interface)	209
	Viewing Resolver Statistics (C-Web Interface)	210
	Viewing Agents (C-Web Interface)	210
	Viewing Agents (C-Web Interface)	210
	Viewing Agent Statistics (C-Web Interface)	211
Chapter 19	Monitoring NTP (SRC CLI)	213
	Viewing NTP Peers (SRC CLI)	213
	Viewing Statistics for NTP (SRC CLI)	214
	Viewing Internal Variables for NTP (SRC CLI)	214
Chapter 20	Monitoring NTP (C-Web Interface)	217
	Viewing NTP Peers (C-Web Interface)	217
	Viewing Statistics for NTP (C-Web Interface)	218
	Viewing NTP Status (C-Web Interface)	218
Chapter 21	Monitoring Redirect Server (SRC CLI)	221
	Viewing Statistics for the Redirect Server (SRC CLI)	221
	Viewing Statistics About Filtered Traffic (SRC CLI)	221
Chapter 22	Monitoring the Redirect Server and Filtered Traffic (C-Web Interface) . .	223
	Viewing Statistics for the Redirect Server (C-Web Interface)	223
	Viewing Information for Filtered Traffic (C-Web Interface)	224
Chapter 23	Troubleshooting Network Connectivity (SRC CLI)	227
	Commands to Troubleshoot Connections to Remote Hosts Overview	227
	Testing Connectivity to Remote Hosts (SRC CLI)	227
	Viewing the Route Information (SRC CLI)	228
	Viewing Routing Table Information (SRC CLI)	229
	Viewing Interface Information (SRC CLI)	229

Chapter 24	Monitoring Network Connectivity (C-Web Interface)	233
	Viewing Information About the Routing Table (C-Web Interface)	233
	Viewing Information About System Interfaces (C-Web Interface)	234
Chapter 25	Monitoring Activity for SRC Components	235
	Monitoring Activity on C Series Controllers	235
	Collecting Data with the Activity Monitor (SRC CLI)	236
	Collecting Data with the Activity Monitor (C-Web Interface)	238
	Viewing Graphs (C-Web Interface)	238
	Viewing Graphs from a Webpage	239
	Viewing Graphs for a Preset Time Period from a Webpage	239
	Viewing Graphs for Specified Time Periods from a Webpage	240

List of Figures

Part 5	Monitoring the SRC Software and the C Series Controller with the C-Web Interface and the SRC CLI	
Chapter 14	Monitoring the System (C-Web Interface)	123
	Figure 1: C-Web Interface for Monitoring System Information	124
	Figure 2: C-Web Interface for Monitoring System Date and Time	125
	Figure 3: C-Web Interface for Monitoring SRC Components Status	125
	Figure 4: C-Web Interface for Monitoring System Boot Messages	126
	Figure 5: C-Web Interface for Monitoring Security Certificates	127
	Figure 6: C-Web Interface for Monitoring System Disk Status	127
	Figure 7: C-Web Interface for Monitoring System Users	128
	Figure 8: C-Web Interface for Monitoring Juniper Networks Database in Community Mode	129
	Figure 9: C-Web Interface for Monitoring Local Juniper Networks Database Statistics	130
	Figure 10: C-Web Interface for Monitoring SRC CLI Settings	131
	Figure 11: C-Web Interface for Monitoring SRC CLI User Permissions	131
Chapter 16	Monitoring SAE Data (C-Web Interface)	169
	Figure 12: C-Web Interface for Monitoring SAE Directory Blacklist	170
	Figure 13: C-Web Interface for Monitoring SAE Services	170
	Figure 14: C-Web Interface for Monitoring SAE Licenses	171
	Figure 15: C-Web Interface for Monitoring SAE Policies	172
	Figure 16: C-Web Interface for Monitoring SAE Device Drivers	173
	Figure 17: C-Web Interface for Monitoring SAE Interfaces	174
	Figure 18: C-Web Interface for Monitoring Equipment Registrations	175
	Figure 19: C-Web Interface for Monitoring Login Registrations	176
	Figure 20: C-Web Interface for Monitoring SAE Threads	177
	Figure 21: C-Web Interface for Monitoring SAE Subscriber Sessions by DN	179
	Figure 22: C-Web Interface for Monitoring SAE Subscriber Sessions by IP Address	180
	Figure 23: C-Web Interface for Monitoring SAE Subscriber Sessions by Login Name	181
	Figure 24: C-Web Interface for Monitoring SAE Subscriber Sessions by Service Name	182
	Figure 25: C-Web Interface for Monitoring SAE Subscriber Sessions by Session ID	183
	Figure 26: C-Web Interface for Monitoring SNMP Statistics of the Directory	184
	Figure 27: C-Web Interface for Monitoring SNMP Statistics of Directory Connections	185
	Figure 28: C-Web Interface for Monitoring SNMP Statistics of Client Licenses	186

	Figure 29: C-Web Interface for Monitoring SNMP Statistics of Virtual Router Licenses	187
	Figure 30: C-Web Interface for Monitoring SNMP Statistics of Local Licenses . .	188
	Figure 31: C-Web Interface for Monitoring SNMP Statistics of Policies	189
	Figure 32: C-Web Interface for Monitoring SNMP Statistics of Server Processes	190
	Figure 33: C-Web Interface for Monitoring SNMP Statistics of RADIUS Server . .	190
	Figure 34: C-Web Interface for Monitoring SNMP Statistics of RADIUS Clients	191
	Figure 35: C-Web Interface for Monitoring SNMP Statistics of Device Drivers . . .	192
	Figure 36: C-Web Interface for Monitoring SNMP Statistics of a Specific Device Driver Type	193
	Figure 37: C-Web Interface for Monitoring SNMP Statistics of Subscriber Sessions and Service Sessions	194
Chapter 18	Monitoring the NIC (C-Web Interface)	207
	Figure 38: C-Web Interface for Monitoring NIC Host Statistics	207
	Figure 39: C-Web Interface for Monitoring NIC Host Process Statistics	208
	Figure 40: C-Web Interface for Monitoring NIC Resolvers	209
	Figure 41: C-Web Interface for Monitoring NIC Resolver Statistics	210
	Figure 42: C-Web Interface for Monitoring NIC Agents	211
	Figure 43: C-Web Interface for Monitoring NIC Agent Statistics	212
Chapter 20	Monitoring NTP (C-Web Interface)	217
	Figure 44: C-Web Interface for Monitoring NTP Peers	217
	Figure 45: C-Web Interface for Monitoring NTP Statistics	218
	Figure 46: C-Web Interface for Monitoring NTP Status	219
Chapter 22	Monitoring the Redirect Server and Filtered Traffic (C-Web Interface) . .	223
	Figure 47: C-Web Interface for Monitoring Redirect Server Statistics	223
	Figure 48: C-Web Interface for Monitoring Filtered Traffic	224
Chapter 24	Monitoring Network Connectivity (C-Web Interface)	233
	Figure 49: C-Web Interface for Monitoring Route Details	233
	Figure 50: C-Web Interface for Monitoring Interface Details	234
Chapter 25	Monitoring Activity for SRC Components	235
	Figure 51: Sample CPU Usage Graph	240
	Figure 52: Sample SAE Heap Usage Graph	241

List of Tables

	About the Documentation	xvii
	Table 1: Notice Icons	xviii
	Table 2: Text Conventions	xviii
Part 2	Using Logging for the SRC Software and C Series Controllers	
Chapter 2	Configuring Logging for SRC Components	7
	Table 3: SAE Categories and Severity Levels	8
	Table 4: Named Severity Levels	18
	Table 5: Examples of Filters for Event Messages	19
	Table 6: SAE Device Filter Formatting Rules for Debug and Info Logs	21
	Table 7: Sample Combinations of Conditions for the device-filter-key Expression	22
Chapter 3	Configuring Logging for SRC Components with the CLI	25
	Table 8: Logrotate Options	32
	Table 9: Options for Specifying How Log Files Are Created	35
Part 4	Using SNMP for Monitoring and Troubleshooting	
Chapter 8	Creating Custom SNMP Monitors	61
	Table 10: Example Table for junisaeRouterTable Object	70
Chapter 11	Understanding Traps	89
	Table 11: Symbols in Performance Traps Tables	89
	Table 12: Performance Traps—SAE	92
	Table 13: Performance Traps—Accounting	94
	Table 14: Performance Traps—Authentication	96
	Table 15: Performance Traps—NIC	97
	Table 16: Performance Traps—Router Drivers	98
	Table 17: Performance Traps—System Management Event	100
	Table 18: Performance Traps—Policy Engine	100
	Table 19: Performance Traps—SRC Redirector	101
	Table 20: Performance Traps—SRC ACP	102
	Table 21: Performance Traps—JPS	102
	Table 22: Performance Traps—Chassis	103
	Table 23: Event Traps	104
	Table 24: Alarm State Transitions	106

Part 5	Monitoring the SRC Software and the C Series Controller with the C-Web Interface and the SRC CLI	
Chapter 12	Monitoring with the SRC CLI and the C-Web Interface	111
	Table 25: Comparison of SRC Monitoring Options	112
Chapter 13	Monitoring the System (SRC CLI)	115
	Table 26: Output Fields for show component	118
Chapter 17	Monitoring and Troubleshooting the NIC (SRC CLI)	195
	Table 27: Commands to Display NIC Statistics	195
	Table 28: Output Fields for show nic statistics process	196
	Table 29: Output Fields for show nic statistics test	197
	Table 30: Output Fields for show nic statistics resolver	199
	Table 31: Output Fields for show nic statistics agent	200
	Table 32: Commands to Display NIC Data	201
	Table 33: Output Fields for show nic data resolver	202
	Table 34: Output Fields for show nic data agent	205
Chapter 19	Monitoring NTP (SRC CLI)	213
	Table 35: Output Fields for show ntp associations command	213

About the Documentation

- SRC Documentation and Release Notes on page xvii
- Audience on page xvii
- Documentation Conventions on page xvii
- Documentation Feedback on page xix
- Requesting Technical Support on page xx

SRC Documentation and Release Notes

For a list of related SRC documentation, see <https://www.juniper.net/documentation/>.

If the information in the latest *SRC Release Notes* differs from the information in the SRC guides, follow the *SRC Release Notes*.

Audience

This documentation is intended for experienced system and network specialists working with routers running Junos OS and JunosE software in an Internet access environment. We assume that readers know how to use the routers, directories, and RADIUS servers that they will deploy in their SRC networks. If you are using the SRC software in a cable network environment, we assume that you are familiar with the PacketCable Multimedia Specification (PCMM) as defined by Cable Television Laboratories, Inc. (CableLabs) and with the Data-over-Cable Service Interface Specifications (DOCSIS) 1.1 protocol. We also assume that you are familiar with operating a multiple service operator (MSO) multimedia-managed IP network.

Documentation Conventions

[Table 1 on page xviii](#) defines the notice icons used in this guide. [Table 2 on page xviii](#) defines text conventions used throughout this documentation.

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: Text Conventions

Convention	Description	Examples
Bold text like this	<ul style="list-style-type: none"> Represents keywords, scripts, and tools in text. Represents a GUI element that the user selects, clicks, checks, or clears. 	<ul style="list-style-type: none"> Specify the keyword exp-msg. Run the install.sh script. Use the pkgadd tool. To cancel the configuration, click Cancel.
Bold text like this	Represents text that the user must type.	user@host# set cache-entry-age cache-entry-age
Fixed-width text like this	Represents information as displayed on your terminal's screen, such as CLI commands in output displays.	<pre>nic-locators { login { resolution { resolver-name /realms/ login/A1; key-type LoginName; value-type SaeId; } } }</pre>

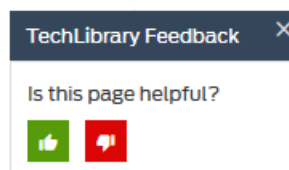
Table 2: Text Conventions (continued)

Regular sans serif typeface	<ul style="list-style-type: none"> Represents configuration statements. Indicates SRC CLI commands and options in text. Represents examples in procedures. Represents URLs. 	<ul style="list-style-type: none"> <code>system ldap server{ stand-alone;</code> Use the <code>request sae modify device failover</code> command with the <code>force</code> option <code>user@host# ...</code> <code>https://www.juniper.net/documentation/software/management/src/api-index.html</code>
<i>Italic sans serif typeface</i>	Represents variables in SRC CLI commands.	<code>user@host# set local-address local-address</code>
Angle brackets	In text descriptions, indicate optional keywords or variables.	Another runtime variable is <gfwif>.
Key name	Indicates the name of a key on the keyboard.	Press Enter.
Key names linked with a plus sign (+)	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
<i>Italic typeface</i>	<ul style="list-style-type: none"> Emphasizes words. Identifies book names. Identifies distinguished names. Identifies files, directories, and paths in text but not in command examples. 	<ul style="list-style-type: none"> There are two levels of access: <i>user</i> and <i>privileged</i>. <i>SRC PE Getting Started Guide</i> <i>o=Users, o=UMC</i> The <i>/etc/default.properties</i> file.
Backslash	At the end of a line, indicates that the text wraps to the next line.	<code>Plugin.radiusAcct-1.class=\net.juniper.smgmt.sae.plugin\RadiusTrackingPluginEvent</code>
Words separated by the symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. (The keyword or variable may be either optional or required.)	<code>diagnostic line</code>

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 system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.

- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide 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 <https://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: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <https://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 <https://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 <https://www.juniper.net/support/requesting-support.html>.

PART 1

Monitoring and Troubleshooting the SRC Software and C Series Controllers

- Overview of Monitoring and Troubleshooting Tools on page 3

CHAPTER 1

Overview of Monitoring and Troubleshooting Tools

- [Monitoring and Troubleshooting Tools Overview on page 3](#)

Monitoring and Troubleshooting Tools Overview

The SRC software provides the following tools to help you monitor and troubleshoot your SRC environment:

- Logging support for SRC components
- System log server on C Series Controllers
- NIC test commands to troubleshoot NIC configuration
- Router simulation to facilitate application testing
- Subscriber simulation to facilitate application testing
- SNMP agent to monitor SRC components as well as system performance. The agent can send data to SNMP network management systems.
- SNMP trap notification to SNMP management systems
- SRC CLI to monitor specified SRC components and C Series Controllers
- C-Web interface to monitor specified SRC components and C Series Controllers

The SRC software also includes various sample and test clients for the dynamic service activator, the SAE remote interface, and the SAE plug-in interface.

Related Documentation

- [Logging for SRC Components Overview on page 7](#)
- [Monitoring with the SRC CLI and the C-Web Interface on page 111](#)
- [SRC Monitoring Options on page 111](#)
- [SNMP Traps Overview on page 83](#)

PART 2

Using Logging for the SRC Software and C Series Controllers

- [Configuring Logging for SRC Components on page 7](#)
- [Configuring Logging for SRC Components with the CLI on page 25](#)
- [Configuring Logging for SRC Components \(C-Web Interface\) on page 39](#)

CHAPTER 2

Configuring Logging for SRC Components

- [Logging for SRC Components Overview on page 7](#)
- [Categories and Severity Levels for Event Messages on page 7](#)
- [Rotating Log Files on page 22](#)

Logging for SRC Components Overview

SRC components and applications generate event messages that you can save in logs—either by writing the messages to text files or by using the system log facilities. You can use these logs to monitor the SRC components and troubleshoot problems.

Each SRC component has its own logging configuration. For example, the license server, the NIC, the SAE, and SNMP each have logging configuration. The C Series Controller includes a system log server that you can configure to manage messages generated on that platform. You can use the CLI and the C-Web interface to configure logging on a C Series Controller and to configure the system log server on a C Series Controller.

When you enable logging to a file, by default SRC components and applications write log files to the `/opt/UMC/<component-directory>/var/log` folder for a component, such as `/opt/UMC/sae/var/log`.

All log files with the file extension `.log` in a `var/log` directory are [“Rotating Log Files” on page 22](#).

Related Documentation

- *C Series Controller Log Server Overview*
- The system log Protocol—draft-ietf-syslog-protocol-16.txt (July 2006 expiration)
- *Configuring the SRC SNMP Agent (SRC CLI)*
- [Configuration Statements for SRC Component Logging on page 25](#)
- [Categories and Severity Levels for Event Messages on page 7](#)

Categories and Severity Levels for Event Messages

In the logging configuration, you can specify a filter for each type of log. This filter can include an expression that defines the *categories* and *severity levels* of event messages

that the software saves. You can also enable network device-specific filtering for service activation engine (SAE) debug and info logs.

Defining Categories

The category of an event message defines the SRC component that generated the event message. If you want to view only event logs in a specific category, you can define a variable `<category>`, which is a text string that matches the name of a category. This variable is not case sensitive. To view the names of categories for event messages, view a log file for one of the default filters.

For example purposes, [Table 3 on page 8](#) lists the SAE logging categories and associated severity levels. These categories are relevant only for loggers configured with the **shared sae configuration logger** statement. The extension refers to loggers that dynamically change their name at runtime. Juniper Networks Customer Service can also provide names of categories for other components, especially for troubleshooting purposes.

Table 3: SAE Categories and Severity Levels

Category	Extension	Severity Level
AAExtIntf		error, debug, debug_8
AAExtIntfIDGenerator		error
AAALdapListener		error, debug
AAARouterDriver		info, error, debug
AAASolicitedJob		info, warning, error, debug
AccessManager		info, error, debug
AccountingFileDict		info, error, debug
AccountingFilePeer		info, error, debug
ACPIntfListener		error, debug
ACRMsg		warning, debug
AddressCtx		info, error, debug
Admin		info, error, debug
AggregateServiceSession		error, debug
AMGroupLDAPListener		info, debug
ASRMsg		warning, debug

Table 3: SAE Categories and Severity Levels (continued)

Category	Extension	Severity Level
Atom		debug
BEEPDebug	-	debug_9
ClassifyDhcp		error, debug
ClassifyInterface		info, error, debug
ClassifyUser		error
Client	/	info, error, debug
ClientMgr	/	info, error, debug
Commands		error
CommunityManager		error, debug
CommunityMember		info, error, debug, debug_9
ConfigChecker		info, error, debug
COPSDecoder		info, debug_9
COPSEncoder		info, debug_10
Core API		error, debug
CustomRadiusAccounting		error, debug
CustomRadiusAuth		error, debug
DataManagerMIData		error
DCImpl		warning, error, debug
DhcpManager		error, debug
DhcpOptions		error
DiameterDriverManager		info, error, debug
DiameterMsgHandler		warning, error, debug, debug_8
DiameterPlacementProcessor		error
DiameterRouterDriver		info, warning, error, debug

Table 3: SAE Categories and Severity Levels (continued)

Category	Extension	Severity Level
DiameterUnsolicitedMsg		info, warning, error, debug
DiscoverDecisionHelper		error
DynRadiusServer		error, debug
EmbeddedPrecedenceProcessor		error, debug_9
EquipRamCache		debug
EquipRegLdapDataManager		info, error, debug
EquipRegLDAPDataManagerConnectionThread		info, error, debug
EventBatch		error, debug
EventPublisher		error, debug
Extension Script		info, error, debug
ExtInterface		info, warning, error, debug
ExtIntf		info, error, debug
FailQueue		error, debug
FeedbackManager		info, error
FileDeleter		info, error, debug
FileRotater		info, error, debug
FileTrackingPluginEventListener		info, error, debug
FlexibleRadiusAuthPluginEventListener		info, error, debug
FlexibleRadiusTrackingPluginEventListener		info, error, debug
FloatingContext		info, error, debug
GateProcessor		error, debug
GenericService		error, debug
GenericSessionJobManager		info, error, debug
HostUtil		error, debug

Table 3: SAE Categories and Severity Levels (continued)

Category	Extension	Severity Level
HttpAttachmentProcessor		info, error, debug
IdleTimeoutObject		debug
InfrastructureServiceSession		error, debug
InterfaceSession		error
InterfaceTimeoutManager		debug
InterimSessionJobManager		info, error, debug
IpInterfaceCtx		info, error, debug
ISEExtIntf		error, debug
ISEPORetriever		error, debug
ISEProvisioningContext		error
ISERouterDriver		info, warning, error, debug
ISESolicitedJob		info, warning, error, debug
JobQueue		info, debug_9
JunoScriptConfHelper	-	info
JunoScriptSubChannelHandler	-	debug, trace
JunosDriverManager		info, error, debug
JunosEDriverManager		info, error, debug
JunosElcc		error, debug
JunoseJob		error, debug
JunosERouterDriver		info, error, debug, debug_9, perf
JunosERouterFactory		info
JunosEXDRRouterDriver		info, error, debug, debug_9, perf
JunosRouterDriver		info, error, debug, debug_9
JunosRouterFactory		info

Table 3: SAE Categories and Severity Levels (continued)

Category	Extension	Severity Level
JunosServiceActivationPoint		error, debug
JunosSessionManager		error, debug
JunosSyslogConfigHandler		info, error, debug
JunosSyslogSubChannelHandler		info, error, debug
KeepAliveTimer		error
LdapAuthenticator		error, debug
LDAPConfManager		error
LicenseCheck		info, error
LicenseLDAPListener		debug
LicenseManager		info, error, debug
LicenseServerClient		info, error, debug
LicenseUtil		debug
LimitNumSubscriberPerIntfAuthPluginListener		debug
ListenerJobManager		debug
LiveSessions	/	info, error, debug
LocalPersistentCheck		error
LoginNameParser		error
LoginRequest		error, debug
LogoutRequest		error, debug
Main		info, debug, panic
MemFailQueue		error, debug
MsgInOps		info, error, debug_8
MsgOutPostUpdateOps		info, debug, debug_8
MsgOutUpdateOps		info, debug

Table 3: SAE Categories and Severity Levels (continued)

Category	Extension	Severity Level
NasPortUtil		debug
NicProxyCompleter		error
OpsBuffer		info, error, debug
PingJob		error, debug_9
PluginManager		info, error, debug
PluginUtil		error
PolicyParameterEngine		debug_8
PolicyDecisionPointLDAPListener		info, debug
PolicyListAugmentingProcessor		info, error, debug
PolicyLists		debug_9
PolicyListSharingProcessor		error, debug
PolicyPPRMsg		warning, error, debug
PolicyServiceSession		error, debug
PolicySharedCtx		info, error, debug
Portal API		error, debug
PostponedScheduledService		debug
PostSyncJob		debug
ProcessorManager		error, debug
ProxyDriverManager		error, debug
ProxyRouterDriver		info, error, debug, debug_9
ProxySessionManager		info, error, panic
PublisherQueue		info, error, debug
QoSAttachmentProcessor		info, error, debug
QosProfileTrackingEntry		info, error, debug

Table 3: SAE Categories and Severity Levels (continued)

Category	Extension	Severity Level
QTPEventListener		info, error, debug
QTPJobQueue		error
QTPThreadPoolThread		error, debug
RadiusAuthPluginEventListener		info, error, debug
RadiusPacket		error, debug
RadiusPeer	-	info, error, debug, debug_9
RadiusPeerGroup	-	info, error, debug
RadiusPluginEventListener		info, error, debug
RadiusSocket		info, error, debug, debug_9
RadiusTrackingPluginEventListener		info, error, debug
ReadyToSyncJob		error, debug_9
RefCounter		error
ReferencedPrecedenceProcessor		error, debug_9
ReferencedProcessor		error, debug
RemotePlugin		info, error, debug
ReplayJob		error, debug
Replicator		info, error, debug, debug_9
Retailer		error, debug
RetailerLdapListener		error, debug
RksEventListener		info, error, debug
RksPluginPublisher		error, debug
RouteConfigPPRMsg		warning, error, debug
RouterComponent		info, error
RouterLDAPListener		debug

Table 3: SAE Categories and Severity Levels (continued)

Category	Extension	Severity Level
RouterRegistry		info, error, debug
RouterScript		info, error, debug
RouterScriptComponent		error
SAEAccessImpl		debug
SAE-AUDIT		info, notice, warning
SchedulingAuthPlugin		info, error, debug
ScriptServiceSession		info, error, debug
ServiceActivator		info, error, debug
ServiceAuthEvent		debug
ServiceFragment		debug
ServiceLDAPDataManager		info, error, debug
ServiceLDAPDataManagerConnectionThread		info, error, debug
ServiceLdapListener		error, debug
ServiceManager		error, debug
ServiceMutexGroup		error
ServiceMutexGroupLdapListener		info, error, debug
ServiceMutexGroupManager		debug
ServiceProfile		error
ServiceProfileLdapListener		error, debug
ServiceSchedule		error
ServiceScheduleLdapListener		info, error, debug
ServiceScheduleManager		debug
ServiceScopeLdapListener		info, error, debug
ServiceSession		info, error, debug

Table 3: SAE Categories and Severity Levels (continued)

Category	Extension	Severity Level
ServiceSessionAttributes		debug
ServiceVrLdapListener		info, error, debug
SessionAudit		notice
SessionFactory		info, error, debug
SessionJob		error
SessionJobManager		info, error, debug
SessionStoreFactory		info, error, debug
SessionStoreImpl	/	info, error, debug
SimRouter		info, warning, error, debug
SimRouterDriver		info, error, debug, debug_9
Slave	/	info, error, debug
SlaveMgr		info, error, debug
SolicitedReplyFactory		error, debug, debug_9
SRQMsg		warning, debug
SSFile		info, error, debug
SSFiles	/	info, error, debug, debug_6
SspAccRadiusPeerMI		info, error
SspAuthRadiusPeerMI		info, error
SspSM		info, error, debug
StateSynchronizer		info, error, debug
Stats		info, error, debug
StoreConfig		info, error, debug
StoreOpIteator		debug, debug_8
SubscriberRef		info, error, debug

Table 3: SAE Categories and Severity Levels (continued)

Category	Extension	Severity Level
SubscriberScheduleLdapListener		error, debug
SubscriberScheduleManager		debug
SubscriptionParser		error
Table		debug
TestMaster		info, error, debug
TestPromo		debug
TimeoutSessionJobManager		info, error, debug
TimePolicyManager		info, error, debug
Transaction		error, debug, debug_9
TransactionManager		debug, debug_9
UCCImpl		error, debug
UnsolicitedMessage		error, debug
UnsolicitedMsgFactory		debug
UnsolicitedTimeoutJob		error, debug
UserLDAPDataManager		info, error, debug
UserLDAPDataManagerConnectionThread		info, error, debug
UserLdapListener		debug
UserManager		error, debug
UserProfile		error, debug
UserProfileManager		debug
UserRamCache		debug
UserSession		info, error, debug
WrapperServiceSession		error, debug

Defining Severity Levels

The event filter provides 128 levels of severity numbered 1–127. A higher number indicates a higher level of severity. Common levels of severity also have a specific name, as shown in [Table 4 on page 18](#).



CAUTION: Enabling the generation of debug log messages has a negative affect on system performance. Do not enable debug log messages unless you are instructed to do so by Juniper Networks Technical Assistance Center (JTAC).

Table 4: Named Severity Levels

Name	Severity Level
logmin	1
debug	10
info	20
notice	30
warning	40
error	50
crit	60
alert	70
emerg	80
panic	90
logmax	127

You can define a severity level as follows:

- Specify an explicit severity. For example:
 - debug—Defines only debug messages
- Specify a minimum severity and a maximum severity. For example:
 - info-warning—Defines messages of minimum severity level of info and a maximum severity level of warning
 - Accept the default minimum (logmin) or maximum (logmax) severity by omitting the minimum or maximum severity. For example:

- info—Defines messages of minimum severity level info and maximum severity level logmax
- -warning—Defines messages of minimum severity level logmin and maximum severity level warning
- Specify no severities to log all event messages.

The syntax for the severity takes the format:

```
[<severity>] | [<minimumSeverity>]-[<maximumSeverity>]
```

Use either the name or the number of a severity level shown in [Table 4 on page 18](#) for the variables in this syntax.

Defining Filters

You specify a filter by defining an expression with the following format:

```
singlematch [,singlematch]*
```

- singlematch—[!] (<category> | ([<category>]/[<severity>] | [<minimumSeverity>]-[<maximumSeverity>]))
- !—Do not log matching events
- <category>—See [“Defining Categories” on page 8](#)
- [<severity>] | [<minimumSeverity>]-[<maximumSeverity>]—See [“Defining Severity Levels” on page 18](#).

The software filters events by evaluating each subexpression in order from left to right. When the software determines that an event message matches a subexpression, the software logs or ignores the message accordingly. You can specify an unlimited number of subexpressions; however, the order in which you specify the subexpressions affects the result.



NOTE: When you configure a filter, you must set appropriate values for categories and severity levels. Otherwise, the commit is not successful and when you commit the changes, a message indicating that the configured filter is invalid is displayed.

[Table 5 on page 19](#) shows some examples of filters.

Table 5: Examples of Filters for Event Messages

Syntax	Event Messages Saved
/	All event messages
/info-	Event messages of level info and above from all categories
Cops/debug	Debug events from COPS category only

Table 5: Examples of Filters for Event Messages (continued)

Syntax	Event Messages Saved
!Cops,/debug	All debug events except those from COPS category
CopsMsg/info-,!CopsMsg,Cops	All messages from COPS category, except those from CopsMsg category with level less than info

Enabling Network Device-Specific Filtering for SAE Debug and Info Logs (SRC CLI)

You can enable network device-specific filtering for SAE debug and info logs based on router name, interface name, or login name by including the **device-filter-key** option under the **shared sae configuration logger** hierarchy level. Enabling network device-specific filtering for SAE debug and info logs reduces the size of the debug and info log files, thereby simplifying troubleshooting and minimizing the impact on SAE performance.

You can enable network device-specific filtering of SAE debug or info logs only if you set the SAE severity level to **debug** or **info**, respectively and then include the **device-filter-key** option under the **shared sae configuration logger** hierarchy level. If you do not set the SAE severity level to **debug** or **info**, but enable network device-specific filtering, then no information is logged in to the SAE debug or info log files, respectively. When using network device-specific filtering, you can add one or more device filters by using an expression that defines certain criteria. Only log events matching the criteria are logged in the SAE debug and info log files. Events that do not match the criteria are not logged in the SAE debug and info log files.



NOTE: SRC network device-specific filtering for SAE debug and info logs is supported on JunosE (COPS) and Junos OS (JSRC) devices.

If the network device-specific filtering for debug and info logs is not enabled, the SAE debug and info loggers display their default behavior. By default, log events that match the subexpression defined by using the **filter** option are logged.

You can configure network device-specific debug and info log filtering by defining an expression with the following format:

deviceFilter [deviceFilter]*

- deviceFilter—OpenQuotes deviceFilterKey CloseQuotes
- deviceFilterKey—SingleDevKey *[Operands SingleDevKey]
- SingleDevKey—varName Equality valName
- varName—"router-name" or "interface-name" or "login-name"
- AlphaNumeric—%x41-5A / %x61-7A / %x30-39 / %x2A
- valName—1*AlphaNumeric
- Equality—"=" or "!="

- Operands—“&” or “|”
- OpenQuotes—“
- CloseQuotes—”

The `deviceFilterKey` expression is composed of one or more `SingleDevKey` expressions. A `SingleDevKey` expression should begin with an open brace and end with a close brace.

The SAE filters events by evaluating each **deviceFilter** in order from left to right. You can specify an unlimited number of device filters; however, the order in which you specify the device filter affects the result. The SAE only logs event messages that match all the criteria.

You specify the **deviceFilter** with the format rules described in [Table 6 on page 21](#).

Table 6: SAE Device Filter Formatting Rules for Debug and Info Logs

Rule	Definition	Meaning
<i>OpenQuotes</i>	“	Denotes an open single or double quotation mark, which is used at the beginning of an expression
<i>CloseQuotes</i>	”	Denotes a close single or double quotation mark, which is used at the end of an expression
<i>Equality</i>	=	Allows logging of only the <i>logevent</i> whose value is equal to the value specified in the <i>valName</i>
	!=	Allows logging of only the <i>logevent</i> whose value is not equal to the value specified in the <i>valName</i>
<i>Operands</i>	&	Allows logging of only the <i>logevent</i> whose value matches the <i>valName</i> value specified in all <i>SingleDevKey</i> expressions in a <i>deviceFilterKey</i>
		Allows logging of the <i>logevent</i> even if its value matches the <i>valName</i> value specified in any one of the <i>SingleDevKey</i> expressions in a <i>deviceFilterKey</i>
<i>varName</i>	<i>router-name</i> or <i>interface-name</i> or <i>login-name</i>	Variable names supported to specify the deviceFilterKey .
<i>valName</i>	<i>AlphaNumeric</i>	Value name associated with each variable name. A <i>valName</i> can contain alphanumeric characters as well as a wildcard character (*).
<i>SingleDevKey</i>	<i>varName Equality</i> <i>valName</i>	Pair of <i>varName</i> and <i>valName</i> associated by using an <i>Equality</i> . Multiple <i>SingleDevKey</i> expressions are associated by using <i>Operands</i> .

[Table 7 on page 22](#) lists some examples of network device-specific filter configurations for SAE debug and info logs.

Table 7: Sample Combinations of Conditions for the device-filter-key Expression

Syntax	Notes
set device-filter-key "router-name=erx440 & interface-name=Fast*"	Uses the AND operator
set device-filter-key "router-name=erx440 interface-name=Fast*"	Uses the OR operator
set device-filter-key "router-name=erx440 & interface-name=Fast* login-name = jane@virneo.net"	Uses the AND and OR operators
set device-filter-key "router-name=erx440 & interface-name=Fast* & login-name = jane*net"	Uses the wildcard character (*) for pattern match
set device-filter-key "router-name=erx440 router-name =erx448"	Uses multiple deviceFilterKey configurations
set device-filter-key "router-name=erx440 & interface-name!=Fast*"	Uses the "not equal to" condition

- Related Documentation**
- [Logging for SRC Components Overview on page 7](#)
 - [SNMP Traps Overview on page 83](#)
 - [Configuring an SRC Component to Store Log Messages in a File \(SRC CLI\) on page 26](#)

Rotating Log Files

Logrotate is a log file management utility that allows you to manage the large number of log files the SRC software generates. Logrotate is essential for managing the disk space on the C Series Controller.

The following SRC components support the logrotate utility:

- Third-Generation Partnership Project (3GPP) gateway
- 3GPP Gy
- SRC Admission Control Plug-in (ACP)
- Activity Monitor
- SNMP agent
- Web application server
- Command-line interface (CLI)
- Diameter server
- Dynamic Service Activator
- IP Multimedia Subsystem (IMS)
- License server
- Monitoring Agent application

- Network information collector (NIC)
- Service activation engine (SAE)
- Subscriber information collector (SIC)
- C-Web interface

You can use logrotate to regularly rotate log files by removing the oldest log files from your system and creating new log files. You can rotate files based on size. You can rotate log files daily, weekly, or monthly. Logrotate can also be used to compress log files. Logrotate usually runs automatically through the Cron utility.

When a new log file is opened to replace an older log file that contains content, a number is appended to the name of the older file. For example, *sae_debug.log.4* is an older log file than *sae_debug.log.1*; whereas *sae_debug.log* is the active log file for SAE.

On C Series Controllers, the software compresses log files and appends the *.gz* suffix; for example, *sae_debug.log.4.gz*. Log files are stored in the */opt/UMC/component-name/var/log* directory; for example, */opt/UMC/sae/var/log*.

You can configure components to send log messages to the system log server on the platform on which the SRC software is running.

If you plan to filter log messages, you should be familiar with severity levels and filters for logging before you configure system logging for a component.

Configuration Overview

You can specify any number of log rotation configuration files on the command line. Configuration options that you specify for a group of log files are considered local options and they override global options of the same name.

Both global and local options can be set in the */etc/logrotate.conf* file. You set global options under the **[edit system logrotate logrotate.conf]** hierarchy level. You set local options for specific logging configuration files such as the */var/log/wtmp* file under the **[edit system logrotate logrotate.conf logfiles name]** hierarchy level. You can also configure log rotation for system and SRC components under the **[edit system logrotate file-name logfiles]** hierarchy level.

Related Documentation

- [Logging for SRC Components Overview on page 7](#)
- [Configuring an SRC Component to Store Log Messages in a File \(SRC CLI\) on page 26](#)
- [Configuration Statements for the Logrotate Utility \(SRC CLI\) on page 30](#)
- [Configuring the Logrotate Utility \(SRC CLI\) on page 32](#)

CHAPTER 3

Configuring Logging for SRC Components with the CLI

- [Configuration Statements for SRC Component Logging on page 25](#)
- [Configuring an SRC Component to Store Log Messages in a File \(SRC CLI\) on page 26](#)
- [Configuring System Logging \(SRC CLI\) on page 28](#)
- [Configuration Statements for the Logrotate Utility \(SRC CLI\) on page 30](#)
- [Configuring the Logrotate Utility \(SRC CLI\) on page 32](#)

Configuration Statements for SRC Component Logging

Use the following configuration statements to configure logging for SRC components. You access these statements from the hierarchy for a component, such as:

- **[edit shared acp configuration]**
- **[edit shared sae configuration]**
- **[edit shared nic scenario *scenario-name*]**
- **[edit snmp agent]**

```
logger name {  
  file-logger {  
    device-filter-key device-filter-key;  
    filter filter ;  
    filename filename ;  
    rollover-filename rollover-filename ;  
    maximum-file-size maximum-file-size ;  
  }  
  syslog-logger {  
    filter filter ;  
    port port ;  
    syslog-host syslog-host ;  
    syslog-facility syslog-facility ;  
    format format ;  
  }  
}
```



NOTE: The `device-filter-key` option is available only on the SAE component.

For detailed information about each configuration statement, see *SRC PE CLI Command Reference*.

**Related
Documentation**

- [Configuring System Logging \(SRC CLI\) on page 28](#)
- [Configuring an SRC Component to Store Log Messages in a File \(SRC CLI\) on page 26](#)
- [Before You Configure Logging for SRC Components on page 39](#)
- [Logging for SRC Components Overview on page 7](#)
- [Categories and Severity Levels for Event Messages on page 7](#)

Configuring an SRC Component to Store Log Messages in a File (SRC CLI)

Use the following statements to configure an SRC component to store log messages in a file:

```
logger name file {  
    device-filter-key device-filter-key;  
    filter filter;  
    filename filename;  
    rollover-filename rollover-filename;  
    maximum-file-size maximum-file-size;  
}
```

If you plan to filter log messages, you should be familiar with severity levels and filters for logging before you configure system logging for a component. See “[Categories and Severity Levels for Event Messages](#)” on page 7.

To configure component logging to a file:

1. From configuration mode, access the configuration statement that configures the logging destination for the component.

```
[edit]  
user@host# component-hierarchy logger name file
```

For example:

```
[edit]  
user@host# edit shared sae configuration logger sae-file-log-1 file
```

```
[edit]  
user@host# edit snmp agent logger snmp-file-log-1 file
```


- Specify the filter to define which event messages the software logs or disregards.

```
[edit shared sae configuration logger sae-file-log-1 file]
user@host# set filter filter
```

If you do not specify a filter, logging to the specified file is disabled.

Filters can specify the logging level, such as debug, or can specify expressions.



NOTE: When you configure a filter, you must set appropriate values for categories and severity levels. Otherwise, the commit is not successful and when you commit the changes, a message indicating that the configured filter is invalid is displayed.

- (Optional) Enable network device-specific filtering for SAE debug and info logs based on router name, interface name, or login name.

For more information about format rules used to define the expression while enabling network device-specific filtering, see the table **SAE Debug Device Filter Formatting Rules** in “Categories and Severity Levels for Event Messages” on page 7.

```
[edit shared sae configuration logger sae-file-log-1 file]
user@host# set device-filter-key device-filter-key
```



NOTE:

- SRC network device-specific filtering for SAE debug and info logs is supported on JunosE (COPS) and Junos OS (JSRC) devices.
- The device-filter-key option is available only on the SAE component.
- You can enable network device-specific filtering of SAE debug and info logs only if you set the SAE severity level to debug and then include the device-filter-key option under the shared sae configuration logger hierarchy level.

- Specify the absolute path of the filename that contains the current log files.

```
[edit shared sae configuration logger sae-file-log-1 file]
user@host# set filename filename
```

Make sure that the user under which the J2EE application server or Web application server runs has write access to this folder. If this user does not have write access to the default folder, configure the component or application to write logs in folders to which the user has write access.

- (Optional) Specify the absolute path of the filename that contains the log history.

```
[edit shared sae configuration logger sae-file-log-1 file]
```

```
user@host# set rollover-filename rollover-filename
```

When the log file reaches the maximum size, the software closes the log file and renames it. If a previous rollover file exists, the software overwrites it. The software then reopens the log file and continues to save event messages in it.



NOTE: On a C Series Controller, log files are rotated according to the settings in the logrotate utility. The logrotate utility specifies how often log files are rotated and whether they are compressed.

6. (Optional) Specify the maximum size of the log file and the rollover file.

```
[edit shared sae configuration logger sae-file-log-1 file]  
user@host# set maximum-file-size maximum-file-size
```



NOTE: The maximum file size is specified in KB. Maximum size of the log file is 10,000,000 KB.

Do not set the maximum file size to a value greater than the available disk space.

**Related
Documentation**

- [Configuring System Logging \(SRC CLI\) on page 28](#)
- [Saving System Log Messages to a File \(SRC CLI\)](#)
- [Sending System Log Messages to Other Servers \(SRC CLI\)](#)
- [Before You Configure Logging for SRC Components on page 39](#)
- [Logging for SRC Components Overview on page 7](#)

Configuring System Logging (SRC CLI)

Use the following statements to configure the SRC software to send log messages to the system logging facility:

```
logger name syslog {  
  filter filter;  
  host host;  
  facility facility;  
  format format;  
  port port;  
}
```

You can configure components to send log messages to the system log server on the platform on which the SRC software is running.

If you plan to filter log messages, you should be familiar with severity levels and filters for logging before you configure system logging for a component. See [“Categories and Severity Levels for Event Messages” on page 7](#).

To configure component logging to the system log server:

1. From configuration mode, access the configuration statement that configures the logging destination for the component. For example:

```
[edit]
user@host# component-hierarchy logger name syslog
```

For example:

```
[edit]
user@host# edit shared sae configuration logger sae-sys-1 syslog
```

```
[edit]
user@host# edit snmp agent logger snmp-sys-1 syslog
```

2. (Optional) Specify the filter to define which event messages the software logs or disregards.

```
[edit shared sae configuration logger sae-sys-1 syslog]
user@host# set filter filter
```

Filters can specify the logging level, such as debug, or can specify expressions.

3. (Optional) Change the IP address or name of a host that collects event messages by means of a standard system logging daemon.

```
[edit shared sae configuration logger sae-sys-1 syslog]
user@host# set host host
```

By default, the host is **loghost** for the system log server on the local host. (Configuration in the `/etc/hosts` file sets **loghost** to **localhost**.)

Make sure that the user under which the J2EE application server or Web application server runs has write access to this folder. If this user does not have write access to the default folder, configure the component or application to write logs in folders to which the user has write access.

4. (Optional) Specify the type of system log in accordance with the system logging protocol, a value of 0–23.

```
[edit shared sae configuration logger sae-sys-1 syslog]
user@host# set facility facility
```

5. (Optional) Specify the Message Format string that indicates how the information in an event message is printed.

```
[edit shared sae configuration logger sae-sys-1 syslog]
user@host# set format format
```

Specify a Message Format string as defined in

<http://docs.oracle.com/javase/1.5.0/docs/api/java/text/MessageFormat.html>

The fields available for events are:

- 0—Time and date of the event
 - 1—Name of the thread generating the event
 - 2—Text message of the event
 - 3—Category of the event
 - 4—Priority of the event
6. (Optional) Specify the port used for system logging, a value of 0–65535.

```
[edit shared sae configuration logger sae-sys-1 syslog]
user@host# set port port
```

Related Documentation

- [Configuring an SRC Component to Store Log Messages in a File \(SRC CLI\) on page 26](#)
- [Saving System Log Messages to a File \(SRC CLI\)](#)
- [Configuration Statements for SRC Component Logging on page 25](#)
- [Before You Configure Logging for SRC Components on page 39](#)
- [Logging for SRC Components Overview on page 7](#)

Configuration Statements for the Logrotate Utility (SRC CLI)

Use the following statements to configure the logrotate utility:

```
system logrotate file-name{
}
system logrotate file-name logfiles name {
  compress;
  delay-compress;
  copy;
  daily;
  weekly;
  monthly;
  rotate rotate;
  size size;
```

```
no-create;
copy-truncate;
if-empty;
missing-ok;
filenames filenames;
shared-scripts;
pre-rotate pre-rotate;
post-rotate post-rotate;
first-action first-action;
last-action last-action;
}
system logrotate file-name logfiles name create {
    default;
    mode mode;
    owner owner;
    group group;
}
system logrotate logrotate.conf {
    compress;
    delay-compress;
    copy;
    daily;
    weekly;
    monthly;
    rotate rotate;
    size size;
    no-create;
    copy-truncate;
    if-empty;
    missing-ok;
}
system logrotate logrotate.conf create {
    default;
    mode mode;
    owner owner;
    group group;
}
system logrotate logrotate.conf logfiles name {
    compress;
    delay-compress;
    copy;
    daily;
    weekly;
    monthly;
    rotate rotate;
    size size;
    no-create;
    copy-truncate;
    if-empty;
    missing-ok;
    filenames filenames;
    shared-scripts;
    pre-rotate pre-rotate;
    post-rotate post-rotate;
    first-action first-action;
```

```

    last-action last-action;
  }
system logrotate logrotate.conf logfiles name create {
  default;
  mode mode;
  owner owner;
  group group;
}

```

- Related Documentation**
- [Logging for SRC Components Overview on page 7](#)
 - [Rotating Log Files on page 22](#)
 - [Configuring the Logrotate Utility \(SRC CLI\) on page 32](#)

Configuring the Logrotate Utility (SRC CLI)

Use the options described in [Table 8 on page 32](#) to configure global and local options for the logrotate utility. You set global options under the **[edit system logrotate logrotate.conf]** hierarchy level. You set local options for specific logging configuration files such as the `/var/log/wtmp` file under the **[edit system logrotate logrotate.conf logfiles *name*]** hierarchy level. You specify log rotation for system and SRC components under the **[edit system logrotate *file-name* logfiles]** hierarchy levels.

Table 8: Logrotate Options

Option	Description
compress	(Optional) Compress old versions of log files in gzip format.
delay-compress	(Optional) Postpone compression of the previous log file until the next rotation cycle. This option takes effect only when used in conjunction with the compress option. Use this option when a program cannot be instructed to close its log file and as a result may continue writing to the previous log file indefinitely.
copy	(Optional) Make a copy of the log file, but do not modify the original log file. Use this option to make a snapshot of the current log file, or when some other utility needs to truncate or parse the file. When you use this option, the create option has no effect because the original log file stays in place.
daily	(Optional) Rotate log files every day.
weekly	(Optional) Rotate log files weekly. This option rotates log files if the current weekday is earlier than the weekday of the last rotation or if more than a week has passed since the last rotation.
monthly	(Optional) Rotate log files monthly. This option rotates log files the first time that logrotate is run in a month (which is normally on the first day of the month).

Table 8: Logrotate Options (continued)

Option	Description
rotate <i>rotate</i>	(Optional) Rotate log files the specified number times before removing them. If set to 0, old versions are removed rather than rotated.
size <i>size</i>	<p>(Optional) Rotate log files when they grow larger than the specified size in bytes.</p> <ul style="list-style-type: none"> • If the size is followed by k, the size is assumed to be in kilobytes. • If the size is followed by M, the size is assumed to be in megabytes. • If the size is followed by G, the size is assumed to be in gigabytes. <p>For example, size 100, size 100k, size 100M, or size 100G are all valid settings for this option.</p> <p>This option is mutually exclusive of the time interval options (daily, weekly, or monthly), and log files are rotated without regard for the last rotation time.</p>
no-create	(Optional) Do not create new log files. This option overrides the settings under the [edit system logrotate logrotate.conf create] , [edit system logrotate logrotate.conf logfiles <i>name</i> create] , and [edit system logrotate <i>file-name</i> logfiles <i>name</i> create] hierarchy levels.
copy-truncate	<p>(Optional) When set, this option copies the active log file to a backup and truncates the active log file. Truncate the original log file in place after creating a copy, instead of moving the old log file and optionally creating a new one. This option is useful when programs cannot be instructed to close their log file and as a result, may continue writing (appending) to the previous log file indefinitely.</p> <p>NOTE: There is a very small time period between copying the file and truncating it, so some logging data might be lost. When you specify this option, the create option has no effect because the old log file stays in place.</p>
if-empty	(Optional) Rotate the log file even if it is empty.
missing-ok	(Optional) If the log file is missing, go on to the next log file without issuing an error message.
filenames <i>filenames</i>	(Optional) Names of the log files to rotate. Separate filenames with a space.

Table 8: Logrotate Options (continued)

Option	Description
shared-scripts	(Optional) Normally, the scripts you specify with the pre-rotate and post-rotate options are run for each log that is rotated and the absolute path to the log file is passed as the first argument to the script. This means a single script may be run multiple times for log file entries that match multiple files. If you specify the shared-scripts option, the scripts are run only once, regardless of how many logs match the wildcard pattern, and the entire pattern is passed to them. However, if none of the logs in the pattern require rotating, the scripts are not run at all. If the scripts exit with an error, the remaining actions are not executed for any log.
pre-rotate <i>pre-rotate</i>	(Optional) The lines between the pre-rotate and endsript (both of which must appear on lines by themselves) are executed (using /bin/sh) before the log file is rotated and only if the log is actually to be rotated. These directives may appear only inside a log file definition. Normally, the absolute path to the log file is passed as the first argument to the script. If the shared-scripts option is specified, the whole pattern is passed to the script.
post-rotate <i>post-rotate</i>	(Optional) The lines between the post-rotate and endsript (both of which must appear on lines by themselves) are executed (using /bin/sh) after the log file is rotated. These directives may appear only inside a log file definition. Normally, the absolute path to the log file is passed as the first argument to the script. If the shared-scripts option is specified, the entire pattern is passed to the script.
first-action <i>first-action</i>	(Optional) The lines between first-action and endsript (both of which must appear on lines by themselves) are executed (using /bin/sh) once before all log files that match the wildcard pattern are rotated, before the pre-rotate script is run, and only if at least one log is to be rotated. These directives may appear only inside a log file definition. The entire pattern is passed to the script as the first argument. If the script exits with an error, no further processing is performed.
last-action <i>last-action</i>	(Optional) The lines between last-action and endsript (both of which must appear on lines by themselves) are executed (using /bin/sh) once after all log files that match the wildcard pattern are rotated, after the post-rotate script is run, and only if at least one log is rotated. These directives may appear only inside a log file definition. The entire pattern is passed to the script as the first argument. If the script exits with an error, only an error message is shown (because this is the last action).

Use the options described in [Table 9 on page 35](#) under the **[edit system logrotate logrotate.conf create]**, **[edit system logrotate logrotate.conf logfiles *name* create]**, and **[edit system logrotate *file-name* logfiles *name* create]** hierarchy levels to specify the permissions, owner, and group of new log files. The default is to use the same mode, owner, and group as the original file.

Table 9: Options for Specifying How Log Files Are Created

Option	Description
default	Create new log files with the same mode, owner, and group as the original file.
mode <i>mode</i>	Create new log files with the specified mode in octal format.
owner <i>owner</i>	Create new log files with the specified owner (username).
group <i>group</i>	Create new log files with the specified group.

- [Configuring the Global Options for the Logrotate Utility on page 35](#)
- [Configuring Log Rotation Options for Specific Logging Configuration Files on page 36](#)
- [Configuring Logging Rotation Options for System and SRC Components \(SRC CLI\) on page 36](#)

Configuring the Global Options for the Logrotate Utility

To configure global options for the logrotate utility:



NOTE: The CLI editing level must be set to expert to set the global options.

1. From configuration mode, access the configuration statement that configures global options for the logrotate utility.

```
[edit]
user@host# edit system logrotate logrotate.conf
```

2. Specify how you want to rotate and compress the log files by setting the desired options listed in [Table 8 on page 32](#). For example, to rotate log files weekly and compress them:

```
[edit system logrotate logrotate.conf]
user@host# set weekly
user@host# set compress
```

3. Specify how you want to create new log files by setting the options listed in [Table 9 on page 35](#). For example, to use the default setting:

```
[edit system logrotate logrotate.conf]
user@host# edit create
user@host# set default
```

Configuring Log Rotation Options for Specific Logging Configuration Files

Use the following procedure to configure log rotation options for specific files such as the `/var/log/wtmp` file.

To configure local options for the logrotate utility:

1. From configuration mode, access the configuration statement that configures local options for the logrotate utility and specify one or more log filenames. Separate log filenames with a space.

```
[edit]
user@host# edit system logrotate logrotate.conf logfiles name
```

2. Specify how you want to rotate and compress the log files by setting the desired options listed in [Table 8 on page 32](#). For example, to rotate log files weekly:

```
[edit system logrotate logrotate.conf logfiles name]
user@host# set weekly
```

3. Specify how you want to create new log files by setting the options listed in [Table 9 on page 35](#). For example, to use the default setting:

```
[edit system logrotate logrotate.conf logfiles name]
user@host# edit create
user@host# set default
```

Configuring Logging Rotation Options for System and SRC Components (SRC CLI)

Options you configure for system and specific SRC components override global and local options of the same name.

To configure log rotation options for the system or for SRC components:

1. From configuration mode, access the configuration statement to configure local options and specify the filename used by the SRC component.

```
[edit]
user@host# edit system logrotate file-name
```

For example, to specify local options for the ACP component:

```
[edit]
user@host# edit system logrotate UMCacp
```

2. Specify the name of one or more log files for which you want to configure compression and rotation options. Separate log filenames with a space.

```
[edit system logrotate UMCacp]  
user@host# edit logfiles name
```

For example, to specify the UMCacp-1 log file:

```
[edit system logrotate UMCacp]  
user@host# edit logfiles UMCacp-1
```

3. Specify how you want to rotate and compress the log files by setting the desired options listed in [Table 8 on page 32](#). For example, to rotate log files weekly:

```
[edit system logrotate UMCacp logfiles UMCacp-1]  
user@host# set weekly
```

4. Specify how you want to create new log files by setting the options listed in [Table 9 on page 35](#). For example, to use the default setting:

```
[edit system logrotate UMCacp logfiles UMCacp-1]  
user@host# edit create  
user@host# set default
```

**Related
Documentation**

- [Logging for SRC Components Overview on page 7](#)
- [Rotating Log Files on page 22](#)
- [Configuration Statements for the Logrotate Utility \(SRC CLI\) on page 30](#)

CHAPTER 4

Configuring Logging for SRC Components (C-Web Interface)

- [Before You Configure Logging for SRC Components on page 39](#)
- [Configuring ACP to Store Log Messages in a File \(C-Web Interface\) on page 39](#)
- [Configuring the SAE to Store Log Messages in a File \(C-Web Interface\) on page 40](#)
- [Configuring NIC to Store Log Messages in a File \(C-Web Interface\) on page 40](#)
- [Configuring the SNMP to Store Log Messages in a File \(C-Web Interface\) on page 41](#)

Before You Configure Logging for SRC Components

Before you configure logging for SRC components, you should be familiar with the logging filters that you can configure. If you use a system logging facility, you should be familiar with the system log protocol. For information about logging filters see [“Logging for SRC Components Overview” on page 7](#).

If you plan to filter log messages, you should be familiar with severity levels and filters for logging before you configure system logging for a component. See [“Categories and Severity Levels for Event Messages” on page 7](#).

Related Documentation

- [Configuring System Logging \(SRC CLI\) on page 28](#)
- [Configuring an SRC Component to Store Log Messages in a File \(SRC CLI\) on page 26](#)
- [Configuration Statements for SRC Component Logging on page 25](#)

Configuring ACP to Store Log Messages in a File (C-Web Interface)

To configure component logging for ACP:

1. Click **Configure**, expand **Shared**, expand **ACP**, and then click **Configuration**.
The Configuration pane appears.
2. From the Create new list, select **Logger**.
3. In the dialog box, type a name for the new logger, and click **OK**.

The name of the logger appears in the side pane and the Logger pane.

4. Expand the logger in the side pane, and then click **File** or **Syslog**.
5. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Related Documentation

- [Configuring an SRC Component to Store Log Messages in a File \(SRC CLI\) on page 26](#)
- [Configuring the SAE to Store Log Messages in a File \(C-Web Interface\) on page 40](#)
- [Configuring NIC to Store Log Messages in a File \(C-Web Interface\) on page 40](#)
- [Configuring SRC ACP \(C-Web Interface\)](#)
- [SRC ACP Overview](#)

Configuring the SAE to Store Log Messages in a File (C-Web Interface)

To configure component logging for SAE:

1. Click **Configure**, expand **Shared**, expand **ACP**, and then click **Configuration**.
The Configuration pane appears.
2. From the Create new list, select **Logger**.
The name of the logger appears in the side pane and the Logger pane.
3. Expand the logger in the side pane, and then click **File** or **Syslog**.
4. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Related Documentation

- [Configuring an SRC Component to Store Log Messages in a File \(SRC CLI\) on page 26](#)
- [Configuring ACP to Store Log Messages in a File \(C-Web Interface\) on page 39](#)
- [Configuring NIC to Store Log Messages in a File \(C-Web Interface\) on page 40](#)
- [Configuring the SNMP to Store Log Messages in a File \(C-Web Interface\) on page 41](#)

Configuring NIC to Store Log Messages in a File (C-Web Interface)

To configure component logging for NIC:

1. Click **Configure**, expand **Shared**, and then click **NIC**.
The NIC pane appears.
2. In the side pane, expand a configuration scenario, such as Scenario:OnePopSharedIp.
3. In the side pane, expand a host, such as Demohost.
The Hosts pane appears.
4. From the Create new list, select **Logger**.

The name of the logger appears in the side pane and the Logger pane.

5. Expand the logger in the side pane, and then click **File** or **Syslog**.
6. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

**Related
Documentation**

- [Configuring an SRC Component to Store Log Messages in a File \(SRC CLI\) on page 26](#)
- [Configuring ACP to Store Log Messages in a File \(C-Web Interface\) on page 39](#)
- [Configuring the SAE to Store Log Messages in a File \(C-Web Interface\) on page 40](#)
- [Configuring the SNMP to Store Log Messages in a File \(C-Web Interface\) on page 41](#)

Configuring the SNMP to Store Log Messages in a File (C-Web Interface)

To configure component logging for SNMP:

1. Click **Configure**, expand **Snmp**, and then click **Agent**.

The Agent pane appears.

2. From the Create new list, select **Logger**.

The name of the logger appears in the side pane and the Logger pane.

3. Expand the logger in the side pane, and then click **File** or **Syslog**.
4. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

**Related
Documentation**

- [Configuring an SRC Component to Store Log Messages in a File \(SRC CLI\) on page 26](#)
- [Configuring ACP to Store Log Messages in a File \(C-Web Interface\) on page 39](#)
- [Configuring the SAE to Store Log Messages in a File \(C-Web Interface\) on page 40](#)
- [Configuring NIC to Store Log Messages in a File \(C-Web Interface\) on page 40](#)

PART 3

Using Simulated Router Drivers and Simulated Subscribers for Testing

- [Configuring a Simulated Router Driver for Testing \(SRC CLI\) on page 45](#)
- [Configuring a Simulated Router Driver for Testing \(C-Web Interface\) on page 49](#)
- [Using Simulated Subscribers for Testing \(SRC CLI\) on page 51](#)

CHAPTER 5

Configuring a Simulated Router Driver for Testing (SRC CLI)

- [Simulated Router Drivers for the SRC Software Overview on page 45](#)
- [Configuring Simulated Router Drivers \(SRC CLI\) on page 45](#)

Simulated Router Drivers for the SRC Software Overview

Simulated router drivers allow you to create subscriber sessions without connecting to a router. You can then use the simulated subscriber sessions to test SAE applications.

The SRC software has a default simulated router driver instance called `default@simJunos`.

Related Documentation

- [Configuring Simulated Router Drivers \(SRC CLI\) on page 45](#)
- [Configuring a Simulated Router Driver for Testing \(C-Web Interface\) on page 49](#)

Configuring Simulated Router Drivers (SRC CLI)

You configure a simulated router in the same way that you configure a real router.

Before you configure a simulated router driver:

- Make sure that you configure an interface classification script for the simulated router.
See [Classification Scripts Overview](#).
- Configure the SAE to instantiate a simulated router driver for each simulated router that you create.
- (Optional) Configure a session store for a simulated router driver. The driver uses the session store to store subscriber sessions, service sessions, and policies.

See [Configuring the Session Store Feature \(SRC CLI\)](#).

Use the following configuration statements to configure simulated router drivers:

```
shared sae configuration driver simulated name {  
  driver-type (junos | junose | pcmm);  
  router-version router-version ;  
}
```

```
driver-address driver-address ;  
transport-router transport-router ;  
}
```

To configure simulated router drivers:

1. From configuration mode, access the configuration statement that configures simulated router drivers. In this sample procedure, west-region is the name of the SAE group, and default@simjunos is the name of the simulated router driver.

```
[edit]  
user@host# edit shared sae group west-region configuration driver simulated  
default@simJunos
```

2. Configure the type of device that the simulated driver simulates.

```
[edit shared sae group west-region configuration driver simulated default@simJunos]  
user@host# set driver-type (junos | junose | pcmm)
```

3. (Optional) Configure the version of the router software to simulate. This is the software version that is sent by the router.

```
[edit shared sae group west-region configuration driver simulated default@simJunos]  
user@host# set router-version router-version
```

4. Configure the IP address of the device driver.

```
[edit shared sae group west-region configuration driver simulated default@simJunos]  
user@host# set driver-address driver-address
```

5. (Optional) Configure the name of a virtual router that is used to connect to the SAE. This value is passed to the router initialization script. It is not supported on the device running Junos OS.

```
[edit shared sae group west-region configuration driver simulated default@simJunos]  
user@host# set transport-router transport-router
```

6. (Optional) Verify the configuration of the simulated driver.

```
[edit shared sae group west-region configuration driver simulated  
default@simJunos]  
  
user@host# show  
  
driver-type junos;  
router-version 8.4;  
driver-address 10.10.90.5;
```

For information about setting up SAE groups, see *Configuring an SAE Group*.

- Related Documentation**
- [Configuring a Simulated Router Driver for Testing \(C-Web Interface\) on page 49](#)
 - [Simulated Router Drivers for the SRC Software Overview on page 45](#)

CHAPTER 6

Configuring a Simulated Router Driver for Testing (C-Web Interface)

- [Configuring a Simulated Router Driver for Testing \(C-Web Interface\) on page 49](#)

Configuring a Simulated Router Driver for Testing (C-Web Interface)

You configure a simulated router in the same way that you configure a real router.

Before you configure a simulated router driver:

- Make sure that you configure an interface classification script for the simulated router.
See [Classification Scripts Overview](#).
- Configure the SAE to instantiate a simulated router driver for each simulated router that you create.
- (Optional) Configure a session store for a simulated router driver. The driver uses the session store to store subscriber sessions, service sessions, and policies.

See [Configuring the Session Store Feature \(SRC CLI\)](#).

To configure simulated router drivers:

1. Click **Configure**, expand **Shared**, expand **SAE**, expand **Configuration**, and then click **Driver**.

The Driver pane appears.

2. From the Create new list, select **Simulated**.
3. In the dialog box, type a name for the new simulated driver, and click **OK**.
The name of the simulated driver appears in the side pane and the Driver pane.
4. Enter information as described in the Help text in the main pane, and click **Apply**.

For information about setting up SAE groups, see *[Configuring an SAE Group](#)*.

Related Documentation

- [Configuring Simulated Router Drivers \(SRC CLI\) on page 45](#)
- [Simulated Router Drivers for the SRC Software Overview on page 45](#)

CHAPTER 7

Using Simulated Subscribers for Testing (SRC CLI)

- [Simulated Subscribers Overview on page 51](#)
- [Commands to Manage Simulated Subscribers on page 51](#)
- [Logging In Simulated Subscribers \(SRC CLI\) on page 52](#)
- [Viewing Subscriber Sessions \(SRC CLI\) on page 55](#)
- [Logging Out Simulated Subscribers \(SRC CLI\) on page 56](#)

Simulated Subscribers Overview

Simulated subscribers allow you to create subscriber sessions without connecting to a router or other device. When developing an application, you can log in as a simulated subscriber to test a portal without a router or a client PC. You can log out from the simulated subscriber session in the same way that you log out from other subscriber sessions.

Related Documentation

- [Logging In Simulated Subscribers \(SRC CLI\) on page 52](#)
- [Logging Out Simulated Subscribers \(SRC CLI\) on page 56](#)
- [Viewing Subscriber Sessions \(SRC CLI\) on page 55](#)
- [Commands to Manage Simulated Subscribers on page 51](#)

Commands to Manage Simulated Subscribers

You can use the following operational mode commands to manage simulated subscribers.

- **request sae login ipv4 authenticated-dhcp**
- **request sae login ipv4 authenticated-interface**
- **request sae login ipv4 unauthenticated-dhcp**
- **request sae login ipv4 unauthenticated-interface**
- **request sae logout dn**

- `request sae logout ip`
- `request sae logout login-name`
- `request sae logout session-id`
- `show sae subscribers`
- `show sae subscribers accounting-user-id`
- `show sae subscribers dn`
- `show sae subscribers ip`
- `show sae subscribers login-name`
- `show sae subscribers session-id`

For detailed information about each command, see the *SRC PE CLI Command Reference*.

Related Documentation

- [Simulated Subscribers Overview on page 51](#)
- [Logging In Simulated Subscribers \(SRC CLI\) on page 52](#)
- [Logging Out Simulated Subscribers \(SRC CLI\) on page 56](#)
- [Viewing Subscriber Sessions \(SRC CLI\) on page 55](#)

Logging In Simulated Subscribers (SRC CLI)

You can log in IPv4 subscribers in the following ways:

- [Logging In Authenticated DHCP Subscribers on page 52](#)
- [Logging In Authenticated Interface Subscribers on page 53](#)
- [Logging In Unauthenticated DHCP Subscribers on page 54](#)
- [Logging In Unauthenticated Interface Subscribers on page 54](#)

Logging In Authenticated DHCP Subscribers

Use the following command to log in simulated IPv4 authenticated DHCP subscribers:

```
request sae login ipv4 authenticated-dhcp virtual-router virtual-router address address
login-name login-name mac-address mac-address <service-bundle service-bundle >
<radius-class radius-class > <interface-name interface-name > <interface-alias
interface-alias > <interface-description interface-description > <nas-port-id nas-port-id
>
```

To log in a simulated IPv4 authenticated DHCP subscriber:

1. Issue the `request sae login ipv4 authenticated-dhcp` command. Specify the `virtual-router`, `address`, `login-name`, and `mac-address` options.

```
user@host> request sae login ipv4 authenticated-dhcp virtual-router virtual-router
address address login-name login-name mac-address mac-address
```

2. (Optional) To specify the service bundle used when logging in the simulated subscriber, use the **service-bundle** option.
3. (Optional) To specify the RADIUS class used when logging in the simulated subscriber, use the **radius-class** option.
4. (Optional) To specify the virtual interface used when logging in the simulated subscriber, use the **interface-name** option.
5. (Optional) To specify the interface description used when logging in the simulated subscriber, use the **interface-alias** option.

If you are simulating JunosE routers, the interface alias is the description that is configured on JunosE routers with the **interface description** command.

6. (Optional) To specify the alternate interface name used when logging in the simulated subscriber, use the **interface-description** option.
7. (Optional) To specify the port identifier of an interface used when logging in the simulated subscriber, use the **nas-port-id** option.

Logging In Authenticated Interface Subscribers

Use the following command to log in simulated IPv4 authenticated interface subscribers:

```
request sae login ipv4 authenticated-interface virtual-router virtual-router address address
login-name login-name <service-bundle service-bundle > <radius-class radius-class >
<interface-name interface-name > <interface-alias interface-alias >
<interface-description interface-description > <nas-port-id nas-port-id >
```

To log in a simulated IPv4 authenticated interface subscriber:

1. Issue the **request sae login ipv4 authenticated-interface** command. Specify the **virtual-router**, **address**, and **login-name** options.

```
user@host> request sae login ipv4 authenticated-interface virtual-router virtual-router
address address login-name login-name
```

2. (Optional) To specify the service bundle used when logging in the simulated subscriber, use the **service-bundle** option.
3. (Optional) To specify the RADIUS class used when logging in the simulated subscriber, use the **radius-class** option.
4. (Optional) To specify the virtual interface used when logging in the simulated subscriber, use the **interface-name** option.
5. (Optional) To specify the interface description used when logging in the simulated subscriber, use the **interface-alias** option.

If you are simulating JunosE routers, the interface alias is the description that is configured on JunosE routers with the **interface description** command.

6. (Optional) To specify the alternate interface name used when logging in the simulated subscriber, use the **interface-description** option.
7. (Optional) To specify the port identifier of an interface used when logging in the simulated subscriber, use the **nas-port-id** option.

Logging In Unauthenticated DHCP Subscribers

Use the following command to log in simulated IPv4 unauthenticated DHCP subscribers:

```
request sae login ipv4 unauthenticated-dhcp virtual-router virtual-router address address  
mac-address mac-address <login-name login-name > <service-bundle service-bundle  
> <radius-class radius-class > <interface-name interface-name > <interface-alias  
interface-alias > <interface-description interface-description > <nas-port-id nas-port-id  
>
```

To log in a simulated IPv4 unauthenticated DHCP subscriber:

1. Issue the **request sae login ipv4 unauthenticated-dhcp** command. Specify the **virtual-router**, **address**, and **mac-address** options.

```
user@host> request sae login ipv4 unauthenticated-dhcp virtual-router virtual-router  
address address mac-address mac-address
```

2. (Optional) To specify the fully-qualified name used to log in the simulated subscriber, use the **login-name** option.
3. (Optional) To specify the service bundle used when logging in the simulated subscriber, use the **service-bundle** option.
4. (Optional) To specify the RADIUS class used when logging in the simulated subscriber, use the **radius-class** option.
5. (Optional) To specify the virtual interface used when logging in the simulated subscriber, use the **interface-name** option.
6. (Optional) To specify the interface description used when logging in the simulated subscriber, use the **interface-alias** option.

If you are simulating JunosE routers, the interface alias is the description that is configured on JunosE routers with the **interface description** command.

7. (Optional) To specify the alternate interface name used when logging in the simulated subscriber, use the **interface-description** option.
8. (Optional) To specify the port identifier of an interface used when logging in the simulated subscriber, use the **nas-port-id** option.

Logging In Unauthenticated Interface Subscribers

Use the following command to log in simulated IPv4 unauthenticated interface subscribers:

```
request sae login ipv4 unauthenticated-interface virtual-router virtual-router interface-name
interface-name <address address > <login-name login-name > <service-bundle
service-bundle > <radius-class radius-class > <interface-alias interface-alias >
<interface-description interface-description > <nas-port-id nas-port-id >
```

To log in a simulated IPv4 authenticated interface subscriber:

1. Issue the **request sae login ipv4 authenticated-interface** command. Specify the **virtual-router** and **interface-name** options.

```
user@host> request sae login ipv4 authenticated-interface virtual-router virtual-router
interface-name interface-name
```

2. (Optional) To specify the IP address from which you log in the simulated subscriber, use the **address** option.
3. (Optional) To specify the fully-qualified name used to log in the simulated subscriber, use the **login-name** option.
4. (Optional) To specify the service bundle used when logging in the simulated subscriber, use the **service-bundle** option.
5. (Optional) To specify the RADIUS class used when logging in the simulated subscriber, use the **radius-class** option.
6. (Optional) To specify the interface description used when logging in the simulated subscriber, use the **interface-alias** option.

If you are simulating JunosE routers, the interface alias is the description that is configured on JunosE routers with the **interface description** command.

7. (Optional) To specify the alternate interface name used when logging in the simulated subscriber, use the **interface-description** option.
8. (Optional) To specify the port identifier of an interface used when logging in the simulated subscriber, use the **nas-port-id** option.

Related Documentation

- [Logging Out Simulated Subscribers \(SRC CLI\) on page 56](#)
- [Viewing Subscriber Sessions \(SRC CLI\) on page 55](#)
- [Commands to Manage Simulated Subscribers on page 51](#)
- [Simulated Subscribers Overview on page 51](#)

Viewing Subscriber Sessions (SRC CLI)

Purpose View all subscriber sessions.

Action user@host> **show sae subscribers**

- Related Documentation**
- [Logging Out Simulated Subscribers \(SRC CLI\) on page 56](#)
 - [Logging In Simulated Subscribers \(SRC CLI\) on page 52](#)

Logging Out Simulated Subscribers (SRC CLI)

You can view subscribers who are logged in and then log out subscribers who are accessible:

- [Logging Out Subscribers by DN on page 56](#)
- [Logging Out Subscribers by IP Address on page 56](#)
- [Logging Out Subscribers by Login Name on page 57](#)
- [Logging Out Subscribers by Session ID on page 57](#)

Logging Out Subscribers by DN

To log out subscribers who are accessible by DN:

1. Issue the **show sae subscribers dn** command to view the subscribers who are accessible by DN.
2. Issue the **request sae logout dn** command to log out all subscribers who are accessible by DN.
3. To log out specific subscribers, use the **filter** option and specify all or part of the DN for the subscribers that you want to log out.

```
user@host> request sae logout dn filter filter
```

4. To specify that no confirmation is requested before the software logs out the subscribers, use the **force** option.

```
user@host> request sae logout dn force  
user@host> request sae logout dn filter filter force
```

Logging Out Subscribers by IP Address

To log out subscribers who are accessible by IP address:

1. Issue the **show sae subscribers ip** command to view the subscribers who are accessible by IP address.
2. Issue the **request sae logout ip** command to log out all subscribers who are accessible by IP address.
3. To log out specific subscribers, use the **filter** option and specify the IP address for the subscribers that you want to log out.

```
user@host> request sae logout ip filter filter
```

4. To specify that no confirmation is requested before the software logs out the subscribers, use the **force** option.

```
user@host> request sae logout ip force  
user@host> request sae logout ip filter filter force
```

Logging Out Subscribers by Login Name

To log out subscribers who are accessible by login name:

1. Issue the **show sae subscribers login-name** command to view the subscribers accessible by login name.
2. Issue the **request sae logout login-name** command to log out all subscribers accessible by login name.
3. To log out specific subscribers, use the **filter** option and specify all or part of the login name for the subscribers that you want to log out.

```
user@host> request sae logout login-name filter filter
```

4. To specify that no confirmation is requested before the software logs out the subscribers, use the **force** option.

```
user@host> request sae logout login-name force  
user@host> request sae logout login-name filter filter force
```

Logging Out Subscribers by Session ID

To log out subscribers who are accessible by session ID:

1. Issue the **show sae subscribers session-id** command to view the subscribers accessible by session ID.
2. Issue the **request sae logout session-id** command to log out all subscribers accessible by session ID.
3. To log out specific subscribers, use the **filter** option and specify all or part of the session ID for the subscribers that you want to log out.

```
user@host> request sae logout session-id filter filter
```

4. To specify that no confirmation is requested before the software logs out the subscribers, use the **force** option.

```
user@host> request sae logout session-id force  
user@host> request sae logout session-id filter filter force
```

**Related
Documentation**

- [Logging In Simulated Subscribers \(SRC CLI\) on page 52](#)
- [Viewing Subscriber Sessions \(SRC CLI\) on page 55](#)
- [Commands to Manage Simulated Subscribers on page 51](#)
- [Simulated Subscribers Overview on page 51](#)

PART 4

Using SNMP for Monitoring and Troubleshooting

- [Creating Custom SNMP Monitors on page 61](#)
- [Configuring SNMP Chassis Alarms on page 73](#)
- [Configuring the SNMP Traps \(SRC CLI\) on page 83](#)
- [Understanding Traps on page 89](#)

CHAPTER 8

Creating Custom SNMP Monitors

- [SNMP Monitoring on C Series Controllers on page 61](#)
- [Configuration Statements for Customized SRC SNMP Monitors on page 63](#)
- [Configuring an SNMP Alarm on a C Series Controller \(SRC CLI\) on page 64](#)
- [Defining an Alarm for an SNMP Monitor That Compares Object Values \(SRC CLI\) on page 65](#)
- [Defining an Alarm to Monitor the Status of an Object \(SRC CLI\) on page 66](#)
- [Defining an Alarm for an SNMP Monitor That Compares Values Against Thresholds \(SRC CLI\) on page 67](#)
- [Defining a Discontinuity Check to Validate Delta Values \(SRC CLI\) on page 68](#)
- [Configuring an SNMPv3 Security Name for SNMP Monitoring \(SRC CLI\) on page 68](#)
- [Defining Events for Which SNMP Sends Notifications \(SRC CLI\) on page 69](#)
- [Defining Events That Set Values for SNMP MIB Objects \(SRC CLI\) on page 69](#)
- [Example: SNMP Monitoring of Multiple MIB Objects on page 70](#)

SNMP Monitoring on C Series Controllers

You can create custom SNMP monitors to detect changes in MIB objects. Use custom monitors to generate an alarm and take action in response to an alarm.

To configure a monitor, you define a condition that when met generates an SNMP notification. You can define a monitor for any single MIB object (of type integer) supported on a C Series Controller. These MIBs include Juniper Networks enterprise-specific objects as well as standard MIB objects.

You can configure the following for custom monitors:

- **Alarms**—Define an alarm condition and an event to generate in response to the alarm.
An alarm identifies the object to be monitored, the frequency with which the monitor retrieves a sample value for the object, and a condition that triggers an event.
- **Events**—Define the type of action (SNMP set or notification) to be taken in response to an alarm condition. If you do not define an event for an alarm, SNMP sends the notifications based on the monitor type.

The SRC software supports the following types of alarm conditions for monitors:

- Boolean test—Compares a sample value with a specified value or range of values.
- Existence test—Monitors when an object appears, disappears, or changes value.
- Threshold test—Monitors when an object's value rises above or falls below specified values.

A monitor supports only one type of alarm condition, or test, at a time. Each alarm can use one of the following sampling methods:

- Absolute value—Uses the actual value of the object.

Existence tests support only absolute values.

- Delta value—Uses the difference between two sample values.

By using the delta value sampling method, you can configure SNMP to detect a discontinuity in values to prevent false alarms caused by the value of a MIB object being reset. At the end of a polling interval before the SNMP agent calculates a delta value, SNMP checks the value of a MIB object called a discontinuity marker. If the value of the discontinuity marker changes, SNMP does not perform the test for the associated condition until the next polling interval.

For alarms that do not have a configured event, SNMP sends the following notifications that are defined in RFC 2981—Event MIB (October 2000):

- Boolean or existence test—`mteTriggerFired`
- Threshold test (rising value)—`mteTriggerRising`
- Threshold test (falling value)—`mteTriggerfalling`

The default configuration for SNMP custom monitors assesses all objects in a MIB branch based on the object identifier specified for the monitor. For this type of monitor, you can configure SNMP notification MIB objects located in the same row as the object that generates the event, as well as for a single object. You can create sophisticated monitors by monitoring an entire branch, then creating notifications for multiple objects.

See the information about SRC MIBs on the Juniper website at <https://www.juniper.net/documentation/software/management/src>.

Also, see information about the `disman` event MIB in RFC 2981—Event MIB (October 2000).

**Related
Documentation**

- [SNMP Traps Overview on page 83](#)
- [Configuring an SNMP Alarm on a C Series Controller \(SRC CLI\) on page 64](#)
- [Configuring an SNMPv3 Security Name for SNMP Monitoring \(SRC CLI\) on page 68](#)
- [Configuration Statements for Customized SRC SNMP Monitors on page 63](#)
- [Example: SNMP Monitoring of Multiple MIB Objects on page 70](#)

Configuration Statements for Customized SRC SNMP Monitors

Use the following configuration statements to configure the SNMP custom monitoring at the [edit] hierarchy level.

```
snmp monitor {
  security-name security-name;
}
snmp monitor alarm name{
  interval interval;
  sample-type (absolute-value | delta-value);
  ignore-startup-alarm;
  event event;
  variable variable;
  strict-oid;
}
snmp monitor alarm name boolean-test {
  comparison (equal | unequal | less | less-or-equal | greater | greater-or-equal);
  value value;
}
snmp monitor alarm name existence-test {
  type (present | absent | changed);
}
snmp monitor alarm name threshold-test {
  rising-threshold rising-threshold;
  falling-threshold falling-threshold;
}
snmp monitor alarm name delta-discontinuity-check {
  variable variable;
}
snmp monitor event namenotification {
  oid oid;
  strict-object [strict-object...];
  wildcarded-object [wildcarded-object...];
}
snmp monitor event name snmp-set {
  variable variable;
  value value;
  strict-oid;
}
```

For detailed information about each configuration statement, see the *SRC PE CLI Command Reference*.

Related Documentation

- [Configuring an SNMP Alarm on a C Series Controller \(SRC CLI\) on page 64](#)
- [Example: SNMP Monitoring of Multiple MIB Objects on page 70](#)
- [Configuring an SNMPv3 Security Name for SNMP Monitoring \(SRC CLI\) on page 68](#)
- [SNMP Monitoring on C Series Controllers on page 61](#)

Configuring an SNMP Alarm on a C Series Controller (SRC CLI)

You can configure SNMP to establish alarms for custom monitors.



NOTE: Configure only one monitor test at a time.

To configure an SNMP alarm:

1. Specify an SNMP username.

See [“Configuring an SNMPv3 Security Name for SNMP Monitoring \(SRC CLI\)” on page 68](#).

2. From configuration mode, access the configuration statements that configures an alarm. For example:

```
[edit]
user@host# edit snmp monitor alarm saeHeapUsage
```

where **saeHeapUsage** is the name of the alarm.

3. Specify the number of seconds between which SNMP samples the value of an object. For example:

```
[edit snmp monitor alarm saeHeapUsage]
user@host# set interval 60
```

4. Specify whether to sample the actual value of the object or the difference between two values. For example, to use the actual of the object:

```
[edit snmp monitor alarm saeHeapUsage]
user@host# set sample-type absolute-value
```

If you set the sample type to **delta-value**, you can configure a discontinuity check. See [“Defining a Discontinuity Check to Validate Delta Values \(SRC CLI\)” on page 68](#).

5. (Optional) Indicate that an alarm not be sent when the alarm is initially activated.

```
[edit snmp monitor alarmsaeHeapUsage]
user@host# set ignore-startup-alarm
```

6. (Optional) Specify the name of the event to be generated in response to an alarm condition. For example:

```
[edit snmp monitor alarm saeHeapUsage]
user@host# set event saeHeapUsageEvent
```

7. Specify the name or object identifier (OID) of the MIB variable to be monitored. For example:

```
[edit snmp monitor alarm saeHeapUsage]
```

```
user@host# set variable juniSdxSaeHeapUsed.0
```

8. (Optional) Specify whether to monitor the SNMP object instance identified by a variable attribute. To monitor the SNMP object instance specified by the variable attribute:

```
[edit snmp monitor alarm saeHeapUsage]
user@host# set strict-oid
```

Do not enable the **strict-oid** option when you monitor a column of an SNMP MIB table. An alarm for a column monitors the column on all entries of the table. If an entry for an object in the column passes an alarm test, an event is generated for that object.

9. Configure a Boolean, existence, or threshold test for the alarm.

Related Documentation

- [Defining an Alarm for an SNMP Monitor That Compares Object Values \(SRC CLI\) on page 65](#)
- [Defining an Alarm to Monitor the Status of an Object \(SRC CLI\) on page 66](#)
- [Defining an Alarm for an SNMP Monitor That Compares Values Against Thresholds \(SRC CLI\) on page 67](#)
- [Configuration Statements for Customized SRC SNMP Monitors on page 63](#)
- [SNMP Monitoring on C Series Controllers on page 61](#)

Defining an Alarm for an SNMP Monitor That Compares Object Values (SRC CLI)

You can configure a monitor to compare a sample value to a specified value or range of values by using one of the following types of comparisons:

- equal
- unequal
- less
- less-or-equal
- greater
- greater-or-equal



NOTE: Configure only one monitor test at a time.

Before you define an alarm type, configure the associated SNMP alarm.

See [“Configuring an SNMP Alarm on a C Series Controller \(SRC CLI\)” on page 64](#).

To configure a monitor to compare a sample to a specified value or range of values:

1. From configuration mode, access the configuration statements that configure SNMP monitoring for a Boolean test. For example:

```
[edit]
user@host# edit snmp monitor alarm saeHeapUsage boolean-test
```

where **saeHeapUsage** is the name of the alarm.

2. Specify the type of Boolean test. For example:

```
[edit snmp monitor alarm saeHeapUsage boolean-test]
user@host# set comparison greater
```

3. Define the value that the test uses. For example:

```
[edit snmp monitor saeHeapUsage boolean-test]
user@host# value 14000000
```

Related Documentation

- [Defining an Alarm to Monitor the Status of an Object \(SRC CLI\) on page 66](#)
- [Defining an Alarm for an SNMP Monitor That Compares Values Against Thresholds \(SRC CLI\) on page 67](#)
- [Configuring an SNMP Alarm on a C Series Controller \(SRC CLI\) on page 64](#)
- [Configuration Statements for Customized SRC SNMP Monitors on page 63](#)
- [SNMP Monitoring on C Series Controllers on page 61](#)

Defining an Alarm to Monitor the Status of an Object (SRC CLI)

You can configure a monitor to identify when a MIB object appears, disappears, or changes value. If the test criteria are met, the test is considered to be successful.



NOTE: Configure only one monitor test at a time.

Before you define an alarm type, configure the associated SNMP alarm.

See “[Configuring an SNMP Alarm on a C Series Controller \(SRC CLI\)](#)” on page 64.

To configure an alarm to monitor the status of an object:

- Specify the type of alarm: present, absent, or changed. For example, for an alarm named existence-alarm:

```
[edit snmp monitor alarm existence-alarm existence-test]
user@host# set type present
```


Related Documentation

- [Defining an Alarm for an SNMP Monitor That Compares Object Values \(SRC CLI\) on page 65](#)
- [Defining an Alarm for an SNMP Monitor That Compares Values Against Thresholds \(SRC CLI\) on page 67](#)
- [Configuring an SNMP Alarm on a C Series Controller \(SRC CLI\) on page 64](#)
- [Configuration Statements for Customized SRC SNMP Monitors on page 63](#)
- [SNMP Monitoring on C Series Controllers on page 61](#)

Defining an Alarm for an SNMP Monitor That Compares Values Against Thresholds (SRC CLI)

You can configure a monitor to compare a sample value for a MIB object to a threshold encountered as the value rises and a threshold encountered as the value falls.



NOTE: Configure only one monitor test at a time.

Before you define an alarm type, configure the associated SNMP alarm.

See [“Configuring an SNMP Alarm on a C Series Controller \(SRC CLI\)” on page 64](#).

To configure an alarm for a monitor that compares a sample value to an upper threshold value and a lower threshold value:

1. Define the upper threshold against which to compare a rising sample value. For example:

```
[edit snmp monitor alarm thresholds threshold-test]
user@host# set rising-threshold 2
```

2. Define the lower threshold against which to compare a falling sample value. For example:

```
[edit snmp monitor alarm threshold-alarm]
user@host# set falling-threshold 1
```

Related Documentation

- [Defining an Alarm for an SNMP Monitor That Compares Object Values \(SRC CLI\) on page 65](#)
- [Defining an Alarm to Monitor the Status of an Object \(SRC CLI\) on page 66](#)
- [Configuring an SNMP Alarm on a C Series Controller \(SRC CLI\) on page 64](#)
- [Configuration Statements for Customized SRC SNMP Monitors on page 63](#)
- [SNMP Monitoring on C Series Controllers on page 61](#)

Defining a Discontinuity Check to Validate Delta Values (SRC CLI)

You can configure a monitor to use a discontinuity check to prevent sending false alarms when the value of the monitored object is reset between two samples.

Use a discontinuity check when the sampling type for a monitor is **delta-value** and the test type is Boolean or threshold. You define a variable, called a discontinuity marker (a MIB object used to validate the delta, or difference, between values). Typically, the marker object is of the TimeTicks, DateAndTime, or Timestamp type.

To define a discontinuity check:

1. Configure an SNMP alarm with the sample type set to **delta-value**.

See [“Configuring an SNMP Alarm on a C Series Controller \(SRC CLI\)” on page 64](#).

2. From configuration mode, access the configuration statements that configures a discontinuity check. For example, for an alarm named ifErrorsDelta:

```
[edit]
user@host# edit snmp monitor alarm ifErrorsDelta delta-discontinuity-check
```

3. Specify the name or object identifier (OID) of the discontinuity marker. For example:

```
[edit snmp monitor alarm sequence-check ifErrorsDelta delta-discontinuity-check]
user@host# set variable ifTable.ifEntry.ifLastChange
```

Related Documentation

- [Defining Events That Set Values for SNMP MIB Objects \(SRC CLI\) on page 69](#)
- [Example: SNMP Monitoring of Multiple MIB Objects on page 70](#)
- [Configuration Statements for Customized SRC SNMP Monitors on page 63](#)
- [SNMP Monitoring on C Series Controllers on page 61](#)

Configuring an SNMPv3 Security Name for SNMP Monitoring (SRC CLI)

To configure an SNMPv3 security name to access a monitored MIB object:

1. From configuration mode, access the configuration statements that configure SNMP monitoring.

```
[edit]
user@host# edit snmp monitor
```

2. Specify an SNMPv3 security name.

```
[edit snmp monitor]
user@host# set security-name your-security-name
```

- Related Documentation**
- [Configuring an SNMP Alarm on a C Series Controller \(SRC CLI\) on page 64](#)
 - [Configuration Statements for Customized SRC SNMP Monitors on page 63](#)
 - [SNMP Monitoring on C Series Controllers on page 61](#)

Defining Events for Which SNMP Sends Notifications (SRC CLI)



NOTE: Do not define an event notification and an SNMP set for the same event.

To define an event for which SNMP sends a notification:

1. From configuration mode, access the configuration statements that configure SNMP event notification and provide a name for the event. For example:

```
[edit]
user@host# edit snmp monitor event routerErrorEvent notification
```

2. Specify the object identifier (OID) object identifier of the notification object. For example:

```
[edit snmp monitor event routerErrorEvent notification]
user@host# set oid junisdxmibs.24.2.1
```

3. (Optional) Allow wildcards in the OID to include instances of subidentifiers that correspond to the monitored object. For example:

```
[edit snmp monitor event routerErrorEvent notification notification]
user@host# set wildcarded-object [junisaeRouterMsgErrors,
junisaeRouterMsgTimeouts]
```

Alternatively, you can configure event notification to use a specific OID.

- Related Documentation**
- [Configuring an SNMP Alarm on a C Series Controller \(SRC CLI\) on page 64](#)
 - [Example: SNMP Monitoring of Multiple MIB Objects on page 70](#)
 - [Configuration Statements for Customized SRC SNMP Monitors on page 63](#)
 - [SNMP Monitoring on C Series Controllers on page 61](#)

Defining Events That Set Values for SNMP MIB Objects (SRC CLI)

You can configure SNMP to set the value of a MIB object in response to an SNMP event.



NOTE: Do not define an event notification and an SNMP set for the same event.

To define an event that sets the value for a MIB variable in response to an SNMP event:

1. From configuration mode, access the configuration statements that configure an SNMP set for an event.

```
[edit]
user@host# edit snmp monitor event event-name snmp-set
```

2. Specify the object identifier (OID) of the MIB variable to set.

```
[edit snmp monitor event event-name snmp-set]
user@host# set oid OID
```

3. Specify the value for the object.

```
[edit snmp monitor event event-name snmp-set]
user@host# set value value
```

4. (Optional) Specify whether the software monitors only the OID specified by the variable option. If you do not set this option, the index of the object triggering the alarm is appended to the variable to be set.

```
[edit snmp monitor event event-name snmp-set]
user@host# set strict-oid
```

Related Documentation

- [Configuring an SNMP Alarm on a C Series Controller \(SRC CLI\) on page 64](#)
- [Example: SNMP Monitoring of Multiple MIB Objects on page 70](#)
- [Configuration Statements for Customized SRC SNMP Monitors on page 63](#)
- [SNMP Monitoring on C Series Controllers on page 61](#)

Example: SNMP Monitoring of Multiple MIB Objects

You can configure SNMP to monitor a column of a MIB table and configure SNMP notifications to include MIB objects located in the same row as the object that generates the event. This example shows how to configure an alarm to generate an event in response to error conditions and send notifications that contain both the number of router errors and router timeouts.

This example uses the `juniSaeRouterTable` shown in [Table 10 on page 70](#). SNMP monitors the `juniSaeRouterMsgErrors` branch, and sends a notification object (`juniSdxMibs.24.2.1`) for the objects in the same row as the object attached to the notification: `juniSaeRouterMsgTimeouts` and `juniSaeRouterMsgErrors`. The monitor generates an event named `routerErrorEvent` for the column `juniSaeRouterMsgErrors`.

Table 10: Example Table for `juniSaeRouterTable` Object

<code>juniSaeRouterClinetId</code>	<code>juniSaeRouterMsgErrors</code>	<code>juniSaeRouterMsgTimeouts</code>
<code>default@router1</code>	100	5

Table 10: Example Table for *juniSaeRouterTable* Object (continued)

juniSaeRouterClnetId	juniSaeRouterMsgErrors	juniSaeRouterMsgTimeouts
default@router2	11	0
default@router3	52	2
...

The following example shows the configuration for this scenario.

```
snmp monitor {
  alarm saeRouterErrors {
    variable juniSaeRouterMsgErrors;
    //strict-oid;
    event routerErrorEvent;
    ...
  }
  event routerErrorEvent notification {
    oid juniSdxMibs.24.2.1
    wildcarded-object [juniSaeRouterMsgErrors,
                      juniSaeRouterMsgTimeouts]
  }
}
```

- Related Documentation
- [SNMP Monitoring on C Series Controllers on page 61](#)
 - [Configuring an SNMP Alarm on a C Series Controller \(SRC CLI\) on page 64](#)
 - [Configuration Statements for Customized SRC SNMP Monitors on page 63](#)

CHAPTER 9

Configuring SNMP Chassis Alarms

- [SNMP Chassis Alarms on a C Series Controller on page 73](#)
- [Configuring SNMP Chassis Alarms \(SRC CLI\) on page 74](#)
- [Defining Alarm Thresholds for Battery Voltage Sensors on page 74](#)
- [Defining Alarm Thresholds for CPU Sensors on page 75](#)
- [Defining Alarm Thresholds for Fan Speed Sensors on page 78](#)
- [Defining Alarm Thresholds for System Temperature Sensors on page 78](#)
- [Defining Alarm Thresholds for Voltage Sensors on page 79](#)

SNMP Chassis Alarms on a C Series Controller

You can configure SNMP to establish built-in chassis alarms that monitor the sensors on C Series Controllers. The chassis alarms are preconfigured SNMP monitors that detect changes in the MIB objects described in Juniper-SDX-CHASSIS-TRAP-MIB (Chassis Trap MIB). The chassis alarms are configured to use the Boolean test condition and absolute value sampling method. Each time you start the SNMP agent and you have enabled chassis alarms, the initial action is to raise the clear trap for all chassis sensors.

You cannot delete chassis alarms, but you can disable them. You can modify the time interval between which SNMP samples the value for the chassis alarms. You can also define the alarm thresholds for each chassis alarm.



NOTE: If you want to use the built-in chassis alarms, you must delete any custom SNMP monitors that you configured to detect changes in the Juniper-SDX-CHASSIS-TRAP-MIB MIB objects.

To configure the chassis alarms, you must set the editing level to expert.

Related Documentation

- [Configuring SNMP Chassis Alarms \(SRC CLI\) on page 74](#)
- [SNMP Monitoring on C Series Controllers on page 61](#)

Configuring SNMP Chassis Alarms (SRC CLI)

To configure SNMP chassis alarms:



NOTE: The chassis alarm is not supported in the virtualized SRC software. Hence, you cannot commit the SRC configurations in the virtualized SRC software if the chassis alarm is enabled.

1. Set the editing level for the CLI to expert.

```
user@host> set cli level expert
```

2. From configuration mode, access the configuration statement that configures the chassis alarms.

```
[edit]
user@host# edit snmp monitor chassis-alarm
```

3. (Optional) Disable all chassis alarms. You cannot delete the chassis alarms.

```
[edit snmp monitor chassis-alarm]
user@host# set disable
```

4. (Optional) Specify the number of seconds between which SNMP samples the value of an object. For example:

```
[edit snmp monitor chassis-alarm]
user@host# set interval 60
```

Related Documentation

- [Defining Alarm Thresholds for Battery Voltage Sensors on page 74](#)
- [Defining Alarm Thresholds for CPU Sensors on page 75](#)
- [Defining Alarm Thresholds for Fan Speed Sensors on page 78](#)
- [Defining Alarm Thresholds for System Temperature Sensors on page 78](#)
- [SNMP Chassis Alarms on a C Series Controller on page 73](#)

Defining Alarm Thresholds for Battery Voltage Sensors

To configure SNMP chassis alarm thresholds for battery voltage sensors:

1. Set the editing level for the CLI to expert.

```
user@host> set cli level expert
```

2. From configuration mode, access the configuration statement that defines the thresholds for battery voltage sensors.


```
[edit]
user@host# edit snmp monitor chassis-alarm battery-voltage
```

3. (Optional) Specify the lower threshold for the minor alarm. For example:

```
[edit snmp monitor chassis-alarm battery-voltage]
user@host# set below-minor 3024
```

4. (Optional) Specify the lower threshold for the major alarm. For example:

```
[edit snmp monitor chassis-alarm battery-voltage]
user@host# set below-major 3008
```

5. (Optional) Specify the lower threshold for the critical alarm. For example:

```
[edit snmp monitor chassis-alarm battery-voltage]
user@host# set below-critical 2992
```

6. (Optional) Specify the upper threshold for the minor alarm. For example:

```
[edit snmp monitor chassis-alarm battery-voltage]
user@host# set over-minor 3744
```

7. (Optional) Specify the upper threshold for the major alarm. For example:

```
[edit snmp monitor chassis-alarm battery-voltage]
user@host# set over-major 3760
```

8. (Optional) Specify the upper threshold for the critical alarm. For example:

```
[edit snmp monitor chassis-alarm battery-voltage]
user@host# set over-critical 3776
```

Related Documentation

- [Configuring SNMP Chassis Alarms \(SRC CLI\) on page 74](#)
- [SNMP Chassis Alarms on a C Series Controller on page 73](#)

Defining Alarm Thresholds for CPU Sensors

- [Defining Alarm Thresholds for CPU Core Voltage Sensors on page 75](#)
- [Defining Alarm Thresholds for CPU DIMM Voltage Sensors on page 76](#)
- [Defining Alarm Thresholds for CPU Temperature Sensors on page 77](#)

Defining Alarm Thresholds for CPU Core Voltage Sensors

To configure SNMP chassis alarm thresholds for CPU core voltage sensors:

1. Set the editing level for the CLI to expert.

```
user@host> set cli level expert
```

2. From configuration mode, access the configuration statement that defines the thresholds for CPU core voltage sensors.

```
[edit]
user@host# edit snmp monitor chassis-alarm cpu-core-voltage
```

3. (Optional) Specify the lower threshold for the minor alarm. For example:

```
[edit snmp monitor chassis-alarm cpu-core-voltage]
user@host# set below-minor 1030
```

4. (Optional) Specify the lower threshold for the major alarm. For example:

```
[edit snmp monitor chassis-alarm cpu-core-voltage]
user@host# set below-major 1020
```

5. (Optional) Specify the lower threshold for the critical alarm. For example:

```
[edit snmp monitor chassis-alarm cpu-core-voltage]
user@host# set below-critical 1008
```

6. (Optional) Specify the upper threshold for the minor alarm. For example:

```
[edit snmp monitor chassis-alarm cpu-core-voltage]
user@host# set over-minor 1728
```

7. (Optional) Specify the upper threshold for the major alarm. For example:

```
[edit snmp monitor chassis-alarm cpu-core-voltage]
user@host# set over-major 1740
```

8. (Optional) Specify the upper threshold for the critical alarm. For example:

```
[edit snmp monitor chassis-alarm cpu-core-voltage]
user@host# set over-critical 1752
```

Defining Alarm Thresholds for CPU DIMM Voltage Sensors

To configure SNMP chassis alarm thresholds for CPU DIMM voltage sensors:

1. Set the editing level for the CLI to expert.

```
user@host> set cli level expert
```

2. From configuration mode, access the configuration statement that defines the thresholds for CPU DIMM voltage sensors.

```
[edit]
user@host# edit snmp monitor chassis-alarm cpu-dimm-voltage
```

3. (Optional) Specify the lower threshold for the minor alarm. For example:

```
[edit snmp monitor chassis-alarm cpu-dimm-voltage]
```

```
user@host# set below-minor 2292
```

4. (Optional) Specify the lower threshold for the major alarm. For example:

```
[edit snmp monitor chassis-alarm cpu-dimm-voltage]
user@host# set below-major 2280
```

5. (Optional) Specify the lower threshold for the critical alarm. For example:

```
[edit snmp monitor chassis-alarm cpu-dimm-voltage]
user@host# set below-critical 2268
```

6. (Optional) Specify the upper threshold for the minor alarm. For example:

```
[edit snmp monitor chassis-alarm cpu-dimm-voltage]
user@host# set over-minor 2832
```

7. (Optional) Specify the upper threshold for the major alarm. For example:

```
[edit snmp monitor chassis-alarm cpu-dimm-voltage]
user@host# set over-major 2844
```

8. (Optional) Specify the upper threshold for the critical alarm. For example:

```
[edit snmp monitor chassis-alarm cpu-dimm-voltage]
user@host# set over-critical 2856
```

Defining Alarm Thresholds for CPU Temperature Sensors

To configure SNMP alarm thresholds for CPU temperature sensors:

1. Set the editing level for the CLI to expert.

```
user@host> set cli level expert
```

2. From configuration mode, access the configuration statement that defines the thresholds for the CPU temperature sensors.

```
[edit]
user@host# edit snmp monitor chassis-alarm cpu-temperature
```

3. (Optional) Specify the upper threshold for the minor alarm. For example:

```
[edit snmp monitor chassis-alarm cpu-temperature]
user@host# set minor 76
```

4. (Optional) Specify the upper threshold for the major alarm. For example:

```
[edit snmp monitor chassis-alarm cpu-temperature]
user@host# set major 78
```

5. (Optional) Specify the upper threshold for the critical alarm. For example:

```
[edit snmp monitor chassis-alarm cpu-temperature]
user@host# set critical 80
```

- Related Documentation**
- [Configuring SNMP Chassis Alarms \(SRC CLI\) on page 74](#)
 - [SNMP Chassis Alarms on a C Series Controller on page 73](#)

Defining Alarm Thresholds for Fan Speed Sensors

To configure SNMP chassis alarm thresholds for fan speed sensors:

1. Set the editing level for the CLI to expert.

```
user@host> set cli level expert
```

2. From configuration mode, access the configuration statement that configures the chassis alarm thresholds for fan speed sensors.

```
[edit]
user@host# edit snmp monitor chassis-alarm fan-speed
```

3. (Optional) Specify the lower threshold for the minor alarm in revolutions per minute. For example:

```
[edit snmp monitor chassis-alarm fan-speed]
user@host# set minor 540
```

4. (Optional) Specify the lower threshold for the major alarm in revolutions per minute. For example:

```
[edit snmp monitor chassis-alarm fan-speed]
user@host# set major 405
```

5. (Optional) Specify the lower threshold for the critical alarm in revolutions per minute. For example:

```
[edit snmp monitor chassis-alarm fan-speed]
user@host# set critical 270
```

- Related Documentation**
- [Configuring SNMP Chassis Alarms \(SRC CLI\) on page 74](#)
 - [SNMP Chassis Alarms on a C Series Controller on page 73](#)

Defining Alarm Thresholds for System Temperature Sensors

To configure SNMP chassis alarm thresholds for system temperature sensors:

1. Set the editing level for the CLI to expert.

```
user@host> set cli level expert
```

2. From configuration mode, access the configuration statement that defines the thresholds for system temperature sensors.

```
[edit]
user@host# edit snmp monitor chassis-alarm system-temperature
```

3. (Optional) Specify the upper threshold for the minor alarm. For example:

```
[edit snmp monitor chassis-alarm system-temperature]
user@host# set minor 76
```

4. (Optional) Specify the upper threshold for the major alarm. For example:

```
[edit snmp monitor chassis-alarm system-temperature]
user@host# set major 78
```

5. (Optional) Specify the upper threshold for the critical alarm. For example:

```
[edit snmp monitor chassis-alarm system-temperature]
user@host# set critical 80
```

Related Documentation

- [Configuring SNMP Chassis Alarms \(SRC CLI\) on page 74](#)
- [SNMP Chassis Alarms on a C Series Controller on page 73](#)

Defining Alarm Thresholds for Voltage Sensors

You can configure alarm thresholds for these voltage sensors:

- 1.8V
- 3.3V
- 5V
- 12V
- -12V

To configure SNMP chassis alarm thresholds for voltage sensors:

1. Set the editing level for the CLI to expert.

```
user@host> set cli level expert
```

2. From configuration mode, access the configuration statement that defines the thresholds for voltage sensors.

```
[edit]
user@host# edit snmp monitor chassis-alarm voltage-sensor
```

For example:

```
[edit]
user@host# edit snmp monitor chassis-alarm voltage-1.8v
```

```
[edit]
user@host# edit snmp monitor chassis-alarm voltage-3.3v
```

```
[edit]
user@host# edit snmp monitor chassis-alarm voltage-5v
```

```
[edit]
user@host# edit snmp monitor chassis-alarm voltage-12v
```

```
[edit]
user@host# edit snmp monitor chassis-alarm voltage-negative12v
```



NOTE: The `voltage-negative12v` option is not available on the C3000 and C5000 Controllers.

3. (Optional) Specify the lower threshold for the minor alarm. For example:

```
[edit snmp monitor chassis-alarm voltage-1.8v]
user@host# set below-minor 1644
```

4. (Optional) Specify the lower threshold for the major alarm. For example:

```
[edit snmp monitor chassis-alarm voltage-1.8v]
user@host# set below-major 1632
```

5. (Optional) Specify the lower threshold for the critical alarm. For example:

```
[edit snmp monitor chassis-alarm voltage-1.8v]
user@host# set below-critical 1620
```

6. (Optional) Specify the upper threshold for the minor alarm. For example:

```
[edit snmp monitor chassis-alarm voltage-1.8v]
user@host# set over-minor 2028
```

7. (Optional) Specify the upper threshold for the major alarm. For example:

```
[edit snmp monitor chassis-alarm voltage-1.8v]
user@host# set over-major 2040
```

8. (Optional) Specify the upper threshold for the critical alarm. For example:

```
[edit snmp monitor chassis-alarm voltage-1.8v]
user@host# set over-critical 2052
```

- Related Documentation**
- [Configuring SNMP Chassis Alarms \(SRC CLI\) on page 74](#)
 - [SNMP Chassis Alarms on a C Series Controller on page 73](#)

CHAPTER 10

Configuring the SNMP Traps (SRC CLI)

- [SNMP Traps Overview on page 83](#)
- [Configuration Statements for the SNMP Traps on page 85](#)
- [Configuring Performance Traps \(SRC CLI\) on page 86](#)
- [Configuring Event Traps \(SRC CLI\) on page 87](#)

SNMP Traps Overview

The SNMP agent provides network management systems with SNMP trap notifications in case of component failure or when critical resources are out of configurable limits. This information is captured in a Management Information Base (MIB).

The SNMP agent can be run on each SRC host. It can monitor any SRC process running on the host and is preconfigured to monitor SRC processes. Additionally, it provides detailed monitoring and configuration of SRC server components.

MIBs

The SNMP agent monitors MIB variables. Most variables measure the performance of the system. Some variables are counters, such as the `saeLogins` variable, which counts the total number of subscriber logins since startup. Some variables are gauges, and their numbers go up and down, such as the `saeHeapUsed` variable, which measures the Java Virtual Machine heap that is currently in use.

A MIB defines a trap type that is associated with many MIB variables. For traps based on counters, the SNMP agent periodically polls each specified variable. It takes the difference between the previous and current values of the variable and compares that difference with the threshold. If the difference has moved up across thresholds, the SNMP agent sends a trap raising an alarm (minor, major, or critical) for the highest threshold crossed to all configured receivers. If the difference has moved down across thresholds, the agent sends a trap clearing the alarm of the lowest threshold crossed.

You can configure the polling interval between samples. If you change the polling interval, also adjust the thresholds. For instance, if the critical threshold for SAE logins is 1,000 and the interval is 60 seconds, then a critical alarm is raised if there are more than 1,000 logins in 60 seconds. But if you change the interval to 600 seconds, then you would need to change the threshold to 10,000 to have the same meaning.

For traps based on gauges, the previous value is not needed; the current value is compared with the thresholds.

In the trap tables, there is a field named R/AV, where R means rate, and AV means absolute value. Rate is used for variables that are counters, and it measures the rate of change of the counter. Absolute value is used for variables that are gauges.

Configuration MIBs

The SRC software has a limited number of MIB variables that can be set, such as variables to shut down or start components.

MIB Structure

The SNMP agent MIB uses the following Juniper Networks MIBs:

- Juniper-SDX-ACP-MIB—SRC ACP MIB
- Juniper-SDX-CHASSIS-MIB—Chassis MIB (for C Series Controllers)
- Juniper-SDX-DES-MIB—Directory eventing system MIB
- Juniper-SDX-DIAMETER-MIB—Diameter component MIB
- Juniper-SDX-GW-MIB—Gateway applications MIB (includes the NIC MIB)
- Juniper-SDX-JPS-MIB—JPS MIB
- Juniper-SDX-LICENSE-MIB—Licensing MIB
- Juniper-SDX-MIB—Main Juniper Networks SDX MIB
- Juniper-SDX-MIBS—Collection of Juniper Networks SDX MIB modules
- Juniper-SDX-POM-MIB—Policy management MIB
- Juniper-SDX-REDIRECTOR-MIB—Redirector MIB
- Juniper-SDX-SAE-MIB—SAE MIB
- Juniper-SDX-TC-MIB—Textual conventions MIB
- Juniper-SDX-TRAP-MIB—SRC trap definition MIB
- Juniper-UNI-SMI—Base SMI MIB

MIB Location

The MIBs are located on the Juniper Networks website at

<https://www.juniper.net/documentation/software/management/src>

Traps

Traps are individual events that the SNMP agent can monitor, such as the number of timeouts or errors that have occurred or connections that have opened or closed. There are two types of traps:

- Performance traps—Traps that poll MIB variables associated with the trap to determine whether a variable has crossed configured thresholds. If the variable crosses a threshold, an alarm is triggered and a trap is sent to the list of configured receivers.
- Event traps—Traps that are sent when an event occurs; for example, when a connection is established or closed.

SNMP Traps and Informs

SNMP notifications can be sent as traps or inform requests. SNMP traps are unconfirmed notifications. SNMP informs are confirmed notifications.

SNMP traps are defined in either standard or enterprise-specific MIBs. The standard and enterprise-specific traps are compiled into the network management software.

With traps, the receiver does not send any acknowledgment when it receives a trap and the sender cannot determine if the trap was received. To increase reliability, SNMP informs are supported in SNMPv3. With an inform, the receiver acknowledges the message with a response.

For information on system logging severity levels for SNMP traps, see “[Categories and Severity Levels for Event Messages](#)” on page 7.

Related Documentation

- [Configuring the SRC SNMP Agent \(SRC CLI\)](#)
- [SAE Performance Traps on page 92](#)
- [Accounting Performance Traps on page 94](#)
- [Authentication Performance Traps on page 96](#)
- [NIC Performance Traps on page 97](#)
- [Router Driver Performance Traps on page 98](#)
- [System Management Performance Traps on page 100](#)
- [Policy Engine Performance Traps on page 100](#)
- [SRC Redirector Performance Traps on page 101](#)
- [SRC ACP Performance Traps on page 101](#)
- [JPS Performance Traps on page 102](#)

Configuration Statements for the SNMP Traps

Use the following configuration statements to configure the SNMP traps and the notification target at the **[edit]** hierarchy level.

```
snmp notify alarm category category-name ...
snmp notify alarm category category-name alarm alarm-name {
    interval interval;
    critical critical;
    major major;
```

```
    minor minor;  
  }  
  snmp notify event category category-name ...  
  snmp notify event category category-name event event-name ...  
  snmp notify target target-name {  
    address;  
    port;  
    community;  
    type (trapv1|trapv2|inform);  
  }
```

For detailed information about each configuration statement, see the *SRC PE CLI Command Reference*.

**Related
Documentation**

- [Configuring Performance Traps \(SRC CLI\) on page 86](#)
- [Configuring Event Traps \(SRC CLI\) on page 87](#)
- [SNMP Traps Overview on page 83](#)

Configuring Performance Traps (SRC CLI)

Use the following configuration statements to configure performance traps:

```
snmp notify alarm category category-name ...  
snmp notify alarm category category-name alarm alarm-name {  
  interval interval;  
  critical critical;  
  major major;  
  minor minor;  
}
```

To configure performance traps:

1. From configuration mode, access the configuration statement that configures the type of performance trap.

```
[edit]  
user@host# edit snmp notify
```

2. Specify the type of trap and the trap name.

```
[edit snmp notify]  
user@host# set alarm category category-name alarm alarm-name
```

You can select from the list of trap types and their associated traps or create new traps.

3. (Optional) Specify the interval at which the variable associated with the trap is polled.

```
[edit snmp notify alarm category category-name alarm alarm-name]
user@host# set interval interval
```

4. Specify the threshold above which a critical alarm is generated.

```
[edit snmp notify alarm category category-name alarm alarm-name]
user@host# set critical critical
```

5. Specify the threshold above which a major alarm is generated.

```
[edit snmp notify alarm category category-name alarm alarm-name]
user@host# set major major
```

6. Specify the threshold above which a minor alarm is generated.

```
[edit snmp notify alarm category category-name alarm alarm-name]
user@host# set minor minor
```

Related Documentation

- [Configuring Event Traps \(SRC CLI\) on page 87](#)
- [Configuration Statements for the SNMP Traps on page 85](#)
- [SAE Performance Traps on page 92](#)
- [Performance Traps on page 89](#)
- [Trap Numbers in Performance Traps on page 90](#)

Configuring Event Traps (SRC CLI)

Use the following configuration statements to configure event traps:

```
snmp notify event category category-name ...
snmp notify event category category-name event event-name ...
```



NOTE: The `systemOperatingFailure` and `diskFailure` traps are not supported in the virtualized SRC software. Hence, you cannot commit the SRC configurations in the virtualized SRC software if these hardware-related traps are set. If you load trap configurations through the LDIF file in the virtualized SRC software, you must delete these traps after loading the trap configurations.

To configure event traps:

1. From configuration mode, access the configuration statement that configures the type of event trap.

```
[edit]  
user@host# edit snmp notify
```

2. Specify the type of trap and the trap name.

```
[edit snmp notify]  
user@host# set event category category-name event event-name
```

You can select from the list of trap types and their associated traps or create new traps.

**Related
Documentation**

- [Configuring Performance Traps \(SRC CLI\) on page 86](#)
- [Configuration Statements for the SNMP Traps on page 85](#)
- [Event Traps on page 103](#)
- [SNMP Traps Overview on page 83](#)

CHAPTER 11

Understanding Traps

- [Performance Traps on page 89](#)
- [Trap Numbers in Performance Traps on page 90](#)
- [Decoding Trap Numbers for Raised Trap Actions on page 91](#)
- [Decoding Trap Numbers for Clear Trap Actions on page 91](#)
- [SRC Performance Traps on page 92](#)
- [Event Traps on page 103](#)
- [Alarm State Transitions on page 106](#)

Performance Traps

Trap tables list all the traps supported by the SNMP agent, the text displayed for each trap, trap thresholds and intervals, and any special notes pertaining to the trap.

[Table 11 on page 89](#) describes the symbols used in the performance traps tables.

Table 11: Symbols in Performance Traps Tables

Symbol	Description
\$S	Severity level of the trap: MINOR, MAJOR, CRITICAL, or CLEAR
\$D	Status data
\$P	Polling interval
\$T	Threshold value
\$A	Trap action; displayed as RAISED or CLEARED
\$L	"Exceeded" if the trap is raised; " is below" if the trap is cleared

SRC performance trap tables contain a trap ID, text displayed, and default values for alarm threshold levels, as well as rate (R) and absolute values (AV) fields.

R/AV

Each performance trap table has a field called R/AV. R means rate, and AV means absolute value.

- Rate is used for variables that are counters. The rate is the difference between the current value of the underlying MIB variable being monitored and its previous value, which was read <interval> time ago. The interval length affects those values that are appropriate for the thresholds; that is, the longer the interval, the larger the thresholds must be. For instance, saeLogins is a counter of the total number of SAE logins. With the default interval of 60 seconds, the critical threshold of 2,000 means that a critical trap is sent if there are more than 2,000 logins within one minute. If you change the interval to 300 seconds (5 minutes), to keep the critical threshold at 2,000 logins a minute, you need to change the threshold to 10,000 (the number of logins in 5 minutes for a rate of 2,000 per minute).
- Absolute value is used for variables that are gauges, and they transition from one alarm threshold level to the next.

Related Documentation

- [SNMP Traps Overview on page 83](#)
- [Trap Numbers in Performance Traps on page 90](#)
- [Configuring Performance Traps \(SRC CLI\) on page 86](#)
- [Accounting Performance Traps on page 94](#)
- [Authentication Performance Traps on page 96](#)

Trap Numbers in Performance Traps

Performance traps contain a trap ID, a severity, and an action. The trap ID, severity, and action are encoded in the trap number to make it easy to configure trap receivers, such as HP OpenView, to color and highlight traps.

Every performance trap has four trap definitions: one for critical, major, and minor severity levels, and one for the clear action. For critical, major, and minor severity levels, the action is raise. For the clear action, there is no severity level, because the severity level is implied by the last raise action for the trap ID.

Severity levels are assigned the following numbers:

- Critical=1
- Major=2
- Minor=3
- Information=5

The `JuniSdxTrapID ::= TEXTUAL-CONVENTION` section in the `Juniper-SDX-TC` MIB lists the trap IDs for all traps. The `Juniper-SDX-TRAP` MIB defines the SDX traps.

You can access the MIBs on the Juniper website at

<https://www.juniper.net/documentation/software/management/src>

**Related
Documentation**

- [Performance Traps on page 89](#)
- [Decoding Trap Numbers for Raised Trap Actions on page 91](#)
- [Decoding Trap Numbers for Clear Trap Actions on page 91](#)

Decoding Trap Numbers for Raised Trap Actions

To decode a trap number for raised trap actions:

- Use the following equation:

$$\text{Trap number} = \text{Trap ID} * 10 + \text{severity}$$

For example, if the trap number is 43, then the trap ID is 4 (saeServiceActivations) and the severity is 3 (MINOR). Therefore, a trap number of 43 means that a MINOR event has occurred for the saeServiceActivations trap.

**Related
Documentation**

- [Decoding Trap Numbers for Clear Trap Actions on page 91](#)
- [Configuring Performance Traps \(SRC CLI\) on page 86](#)
- [Trap Numbers in Performance Traps on page 90](#)
- [Performance Traps on page 89](#)

Decoding Trap Numbers for Clear Trap Actions

To decode a trap number for clear trap actions:

- Use the following equation:

$$\text{Trap number} = \text{Trap ID} * 10$$

For example, if the trap number is 250, then the trap ID is 25 (saeAccPendingRequests). Therefore, a trap number of 250 means that the saeAccPendingRequests alarm has been cleared.

**Related
Documentation**

- [Decoding Trap Numbers for Raised Trap Actions on page 91](#)
- [Configuring Performance Traps \(SRC CLI\) on page 86](#)
- [Trap Numbers in Performance Traps on page 90](#)
- [Performance Traps on page 89](#)

SRC Performance Traps

The following SRC performance trap tables are available:

- [SAE Performance Traps on page 92](#)
- [Accounting Performance Traps on page 94](#)
- [Authentication Performance Traps on page 96](#)
- [NIC Performance Traps on page 97](#)
- [Router Driver Performance Traps on page 98](#)
- [System Management Performance Traps on page 100](#)
- [Policy Engine Performance Traps on page 100](#)
- [SRC Redirector Performance Traps on page 101](#)
- [SRC ACP Performance Traps on page 101](#)
- [JPS Performance Traps on page 102](#)
- [Chassis Performance Traps on page 103](#)

SAE Performance Traps

Table 12 on page 92 lists the performance traps for the SAE.

Table 12: Performance Traps—SAE

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)			Interval (sec)	R/AV
			Critical	Major	Minor		
saeHeapUsed	1	\$S:SAE:\$D% of Java VM heap is in use. This \$L the threshold of \$T %:.\$A	95	90	80	60	AV
saeLogins	2	\$S:SAE:During the last \$Ps, \$D logins occurred. This \$L the threshold of \$T logins:.\$A	2000	1000	400	60	R
saeLogouts	3	\$S:SAE:During the last \$Ps, \$D logouts occurred. This \$L the threshold of \$T logouts:.\$A	2000	1000	400	60	R

Table 12: Performance Traps—SAE (continued)

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)			Interval (sec)	R/AV
			Critical	Major	Minor		
saeServiceActivations	4	\$S:SAE:During the last \$Ps, \$D services were activated. This \$L the threshold of \$T service activations.:\$A	2000	1000	500	60	R
saeServiceDeactivations	5	\$S:SAE:During the last \$Ps, \$D services were deactivated. This \$L the threshold of \$T service deactivations.:\$A	2000	1000	500	60	R
saeCurrentUsers	6	\$S:SAE:The number of user sessions is \$D. This \$L the threshold of \$T users sessions.:\$A	18000	14000	12000	60	AV
saeUserNumberLicense	7	\$S:SAE:\$D% of the available licenses are in use. This \$L the threshold of \$T.:\$A	99	95	90	60	AV
saeUserLicenseExpiry	8	\$S:SAE:The SAE license is about to expire in \$D days. This \$L the threshold of \$T.:\$A	1	10	14	3500	AV
saeClientLicExpiry	12	\$S:SAE:The client has consumed \$D% of its available license. This \$L the threshold of \$T.:\$A	90	70	40	900	AV
saeVtaFailQueueSize	14	{0}:SAE:The SAE VTA Fail Queue Size is {1} MB.	5000	3000	1000	120	AV

- See Also**
- [Performance Traps on page 89](#)
 - [Trap Numbers in Performance Traps on page 90](#)
 - [Configuring Performance Traps \(SRC CLI\) on page 86](#)

Accounting Performance Traps

Table 13 on page 94 lists the performance traps for accounting.

Table 13: Performance Traps—Accounting

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)			Interval (sec)	R/AV
			Critical	Major	Minor		
saeAccInvalidServerAddresses	20	\$S:SAE RADIUS Accounting Client:During the last \$Ps, \$D invalid server address errors occurred. This \$L the threshold of \$T invalid server address errors.:\$A	5	2	1	60	R
saeAccRoundTripTime	21	\$S:SAE RADIUS Accounting Client:The round trip message time is \$Dms. This \$L the threshold of \$Tms.:\$A	2250	1500	750	60	AV
saeAccRetransmissions	22	\$S:SAE RADIUS Accounting Client:During the last \$Ps, \$D retransmissions occurred. This \$L the threshold of \$T retransmissions.:\$A	5	2	1	60	R
saeAccMalformedResponses	23	\$S:SAE RADIUS Accounting Client:During the last \$Ps, \$D malformed responses occurred. This \$L the threshold of \$T malformed responses.:\$A	5	2	1	60	R

Table 13: Performance Traps—Accounting (continued)

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)			Interval (sec)	R/AV
			Critical	Major	Minor		
saeAccBadAuthenticators	24	\$S:SAE RADIUS Accounting Client:During the last \$Ps, \$D bad authenticator error occurred. This \$L the threshold of \$T bad authenticators errors.: \$A	5	2	1	60	R
saeAccPendingRequests	25	\$S:SAE RADIUS Accounting Client:The number of pending requests is \$D. This \$L the threshold of \$T pending requests: \$A	50	25	10	60	AV
saeAccTimeouts	26	\$S:SAE RADIUS Accounting Client:During the last \$Ps, \$D timeouts occurred. This \$L the threshold of \$T timeouts.: \$A	30	20	10	60	R
saeAccUnknownTypes	27	\$S:SAE RADIUS Accounting Client:During the last \$Ps, \$D unknown type errors occurred. This \$L the threshold of \$T unknown type errors.: \$A	30	20	10	60	R
saeAccPacketsDropped	28	\$S:SAE RADIUS Accounting Client:During the last \$Ps, \$D packets were dropped. This \$L the threshold of \$T dropped packets.: \$A	30	20	10	60	AV

- See Also**
- [Performance Traps on page 89](#)
 - [Trap Numbers in Performance Traps on page 90](#)

- [Configuring Performance Traps \(SRC CLI\) on page 86](#)

Authentication Performance Traps

[Table 14 on page 96](#) lists the performance traps for authentication.

Table 14: Performance Traps—Authentication

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)				R/AV
			Critical	Major	Minor	Interval(sec)	
saeAuthInvalidServerAddresses	40	\$S:SAE RADIUS Authentication Client:During the last \$Ps, \$D invalid server address errors occurred. This \$L the threshold of \$T invalid server address errors.:\$A	10	5	1	60	AV
saeAuthRoundTripTime	41	\$S:SAE RADIUS Authentication Client:The round trip message time is \$Dms. This \$L the threshold of \$Tms:\$A	2250	1500	750	60	R
saeAuthAccessRetransmissions	42	\$S:SAE RADIUS Authentication Client:During the last \$Ps, \$D retransmissions occurred. This \$L the threshold of \$T retransmissions.:\$A	5	2	1	60	R
saeAuthMalformed AccessResponses	43	\$S:SAE RADIUS Authentication Client:During the last \$Ps, \$D malformed responses occurred. This \$L the threshold of \$T malformed responses.:\$A	5	2	1	60	R
saeAuthBadAuthenticators	44	\$S:SAE RADIUS Authentication Client:During the last \$Ps, \$D bad authenticators errors occurred. This \$L the threshold of \$T.:\$A	5	2	1	60	
saeAuthPendingRequests	45	\$S:SAE RADIUS Authentication Client:The number of pending requests is \$D. This \$L the threshold of \$T pending requests:\$A	50	25	10	60	AV
saeAuthTimeouts	46	\$S:SAE RADIUS Authentication Client:During the last \$Ps, \$D timeouts occurred. This \$L the threshold of \$T timeouts.:\$A	5	2	1	60	R

Table 14: Performance Traps—Authentication (continued)

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)				R/AV
			Critical	Major	Minor	Interval(sec)	
saeAuthUnknownTypes	47	\$S:SAE RADIUS Authentication Client:During the last \$Ps, \$D unknown type errors occurred. This \$L the threshold of \$T unknown type errors.:\$A	5	2	1	60	R
saeAuthPacketsDropped	48	\$S:SAE RADIUS Authentication Client:During the last \$Ps, \$D packets were dropped. This \$L the threshold of \$T dropped packets.:\$A	5	2	1	60	R

- See Also**
- [Performance Traps on page 89](#)
 - [Trap Numbers in Performance Traps on page 90](#)
 - [Configuring Performance Traps \(SRC CLI\) on page 86](#)

NIC Performance Traps

Table 15 on page 97 lists the performance traps for NIC.

Table 15: Performance Traps—NIC

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)				R/AV
			Critical	Major	Minor	Interval(sec)	
nicHostReslvErrors	230	\$S:NIC Host: During the last \$Ps, the number of resolution errors that occurred is \$D. This \$L is the threshold of \$T errors.:\$A	10	5	1	60	R
nicHostAvgReslvTime	231	\$S:NIC Host: During the last \$Ps, the average time this NIC Host spent on resolutions is \$Dms. This \$L the threshold of \$Tms.:\$A	1000	500	250	60	R

- See Also**
- [Performance Traps on page 89](#)
 - [Trap Numbers in Performance Traps on page 90](#)
 - [Configuring Performance Traps \(SRC CLI\) on page 86](#)

Router Driver Performance Traps

Table 16 on page 98 lists the performance traps for router drivers.

Table 16: Performance Traps—Router Drivers

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)				R/AV
			Critical	Major	Minor	Interval(sec)	
routerMsgErrors	190	\$S:SAE Router Driver (\$juniSaeRouterClientId):During the last \$Ps, \$D router errors occurred. This \$L the threshold of \$T errors.:\$A	10	5	1	60	R
routerMsgTimeouts	191	\$S:SAE Router Driver (\$juniSaeRouterClientId):During the last \$Ps, \$D router timeouts occurred. This \$L the threshold of \$T timeouts.:\$A	10	5	1	60	R
routerAvgJobQTime	192	\$S:SAE Router Driver (\$juniSaeRouterClientId):During the last \$Ps, the average time that incoming router messages waited to be processed is \$Dms. This \$L the threshold of \$Tms.:\$A	500	250	100	60	R
routerJobQLength	193	\$S:SAE Router Driver (\$juniSaeRouterClientId):The number of unprocessed incoming router messages is \$D. This \$L the threshold of \$T messages.:\$A	2500	500	100	60	AV
routerJobQAge	194	\$S:SAE Router Driver (\$juniSaeRouterClientId):The oldest unprocessed router message has been waiting for \$Dms. This \$L the threshold of \$Tms.:\$A	30000	10000	5000	60	AV
routerAvgAddTime	195	\$S:SAE Router Driver (\$juniSaeRouterClientId): During the last \$Ps, the average time (in milliseconds) this router driver spent handling 'object added' notifications is \$Dms. This \$L the threshold of \$Tms.:\$A	1000	500	100	60	R

Table 16: Performance Traps—Router Drivers (continued)

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)				R/AV
			Critical	Major	Minor	Interval(sec)	
routerAvgChgTime	196	\$S:SAE Router Driver (\$juniSaeRouterClientId): During the last polling interval, the average time (in milliseconds) this router driver spent handling 'object changed' notifications is \$Dms. This \$L the threshold of \$Tms.:\$A	1000	500	100	60	R
routerAvgDelTime	197	\$S:SAE Router Driver (\$juniSaeRouterClientId): During the last polling interval, the average time (in milliseconds) this router driver spent handling 'object deleted' notifications is \$Dms. This \$L the threshold of \$Tms.:\$A	1000	500	100	60	R
routerStateOutOfSynch	198	{O}:SAE Router Driver:REMOVE DEC message timed out. ERX Router and the router driver are in inconsistent state. Either COPS connection bounce or SAE restart is required to trigger the sync request : {1}	50	10	1	30	AV

- See Also**
- [Performance Traps on page 89](#)
 - [Trap Numbers in Performance Traps on page 90](#)
 - [Configuring Performance Traps \(SRC CLI\) on page 86](#)

System Management Performance Traps

Table 17 on page 100 lists the performance traps for system management event.

Table 17: Performance Traps—System Management Event

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)				R/AV
			Critical	Major	Minor	Interval(sec)	
agentLdapLimitReached	113	\$S: Ldap: The Ldap Limit has been reached: \$D entries, during the last \$Ps. This \$L the threshold of \$T entries.:\$A.	100% of MAX	95% of MAX	90% of MAX	30	AV

- See Also**
- [Performance Traps on page 89](#)
 - [Trap Numbers in Performance Traps on page 90](#)
 - [Configuring Performance Traps \(SRC CLI\) on page 86](#)

Policy Engine Performance Traps

Table 18 on page 100 lists the performance traps for policy engine.

Table 18: Performance Traps—Policy Engine

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)				R/AV
			Critical	Major	Minor	Interval(sec)	
penAvgPGModProcTime	150	\$S:Policy Engine:The average policy group modification processing time is \$D ms. This \$L the threshold of \$T ms.:\$A	200	500	1000	60	AV
penAvgICModProcTime	151	\$S:Policy Engine:The average interface classifier modification processing time is \$D ms. This \$L the threshold of \$T ms.:\$A	200	500	1000	60	AV

Table 18: Performance Traps—Policy Engine (continued)

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)				R/AV
			Critical	Major	Minor	Interval(sec)	
pdpErrors	152	\$S:Policy Decision Point:During the last \$Ps, \$D errors occurred. This \$L the threshold of \$T PDP errors.:\$A	10	5	1	30	R

- See Also**
- [Performance Traps on page 89](#)
 - [Trap Numbers in Performance Traps on page 90](#)
 - [Configuring Performance Traps \(SRC CLI\) on page 86](#)

SRC Redirector Performance Traps

Table 19 on page 101 lists the performance traps for SRC redirector.

Table 19: Performance Traps—SRC Redirector

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)				R/AV
			Critical	Major	Minor	Interval(sec)	
redirGBLimitReached	170	\$S:SDX Redirector:During the last \$Ps, the global bucket limit has been reached for \$D times. This \$L the threshold of \$T times.:\$A	3	2	1	900	R

- See Also**
- [Performance Traps on page 89](#)
 - [Trap Numbers in Performance Traps on page 90](#)
 - [Configuring Performance Traps \(SRC CLI\) on page 86](#)

SRC ACP Performance Traps

Table 20 on page 102 lists the performance traps for the SRC-Admission Control Plug-In (SRC ACP) application.

Table 20: Performance Traps—SRC ACP

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)				R/AV
			Critical	Major	Minor	Interval(sec)	
acpHeapUsed	280	\$S:ACP:\$D% of Java VM heap is in use. This \$L the threshold of \$T%::\$A	95%	90%	80%	60	AV

- See Also**
- [Performance Traps on page 89](#)
 - [Trap Numbers in Performance Traps on page 90](#)
 - [Configuring Performance Traps \(SRC CLI\) on page 86](#)

JPS Performance Traps

Table 21 on page 102 lists the performance traps for the Juniper Policy Server (JPS).

Table 21: Performance Traps—JPS

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)				R/AV
			Critical	Major	Minor	Interval(sec)	
jpsHeapUsed	250	\$S:JPS:\$D% of Java VM heap is in use. This \$L the threshold of \$T%::\$A	95%	90%	80%	60	AV
jpsCmtsAvgSyncTime	251	\$S:JPS:During the last \$Ps, the average time this JPS spent on CMTS synchronizations is \$Dms. This \$L the threshold of \$Tms::\$A	900s	600s	200s	60	R
jpsCmtsAvgDecTime	252	\$S:JPS:During the last \$Ps, the average time the CMTS connection spent on successfully completed DEC/RPT transactions is \$Dms. This \$L the threshold of \$Tms::\$A	3s	2s	1s	60	R
jpsMsgHdlrProcTime	253	\$S:JPS:During the last \$Ps, the average time the JPS message handler spent on message handling is \$Dms. This \$L the threshold of \$Tms::\$A	10s	5s	2s	60	R
jpsMsgFlowProcTime	254	\$S:JPS:During the last \$Ps, the average time the JPS message flow spent on message handling is \$Dms. This \$L the threshold of \$Tms::\$A	30s	15s	6s	60	R

Table 21: Performance Traps—JPS (continued)

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)				R/AV
			Critical	Major	Minor	Interval(sec)	
jpsMsgFlowDroppedMsgs	255	\$S:JPS:During the last \$Ps, the number of messages dropped by a JPS message flow is \$D. This \$L the threshold of \$T.:\$A	1000	100	1	60	R

- See Also**
- [Performance Traps on page 89](#)
 - [Trap Numbers in Performance Traps on page 90](#)
 - [Configuring Performance Traps \(SRC CLI\) on page 86](#)

Chassis Performance Traps

Table 22 on page 103 lists the performance traps for chassis events.

Table 22: Performance Traps—Chassis

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)				R/AV
			Critical	Major	Minor	Interval (sec)	
diskUsage	302	\$S:diskUsage: directory (juniSdxDiskPath) uses up to (juniSdxDiskUsedPercentage) of disk space. This exceeded (THRESHOLD).:RAISE	95% of MAX	90% of MAX	80% of MAX	60	AV

- See Also**
- [Performance Traps on page 89](#)
 - [Trap Numbers in Performance Traps on page 90](#)
 - [Configuring Performance Traps \(SRC CLI\) on page 86](#)

Event Traps

Table 23 on page 104 lists the event traps.

Table 23: Event Traps

Trap Event	Trap ID	Text Displayed
saeLicenseNetworkCapacity	9	\$S:SAE:The total number of sum-weighted line cards allocated in this SRC network is \$LINE_CARD_NUMBER (\$THRESHOLD_PERCENTAGE)%. This \$L the network ERX capacity threshold of \$T sum-weighted line cards.: \$A
saeServiceSessionLicense	11	\$S:LICENSE SERVER:\$SERVICE_SESSIONS (\$SERVICES_PERCENTAGE%) of the available licensed service sessions are in use.: \$A
vtaEjbConnectionStatus	13	INFORMATION:SAE:Vta EJB plug-in connection changes its status:RAISE
sspluginSyncFailQueueSize	15	<p>When the trap is raised, the text displayed is:</p> <p>SS Plugin:{plugin-name}: Mem Fail queue Size during Synchronization exceeded:RAISE</p> <p>When the trap is cleared, the text displayed is:</p> <p>SS Plugin:{plugin-name}: Mem Fail queue Size during Synchronization exceeded:CLEAR</p> <p>NOTE: If the SAE is restarted after the trap is raised, then the SRC software does not send the clear trap for the already raised trap.</p>
ldapSizeLimitExceeded	16	<p>CRITICAL:\$REASON:LDAP Size limit exceeded:RAISE</p> <p>NOTE: This trap is supported only for CLI and SAE components.</p>
routerConnClosed	211	<p>When juniSaeRouterUseFailOver is FALSE:</p> <ul style="list-style-type: none"> INFORMATION:SAE Router Driver: The router connection to \$juniSaeRouterClientId has been closed.:RAISE <p>When juniSaeRouterUseFailOver is TRUE:</p> <ul style="list-style-type: none"> INFORMATION:SAE Router Driver:The router connection to \$juniSaeRouterClientId has been closed and redirected to \$juniSaeRouterFailOverIp:\$juniSaeRouterFailOverPort:RAISE
routerConnDown	212	INFORMATION:SAE Router Driver:The router connection to \$juniSaeRouterClientId went down.:RAISE
routerConnRejected	213	INFORMATION:SAE Router Driver:The router connection from \$juniSaeRouterClientId has been rejected.:RAISE
routerConnUp	210	INFORMATION:SAE Router Driver:A new router connection was established with \$juniSaeRouterClientId.:RAISE
routerConfOutOfSynch	214	<p>When the trap is raised, the text displayed is:</p> <ul style="list-style-type: none"> INFORMATION:SAE Router Driver: The configured state of router \$juniSaeRouterClientId is out of synch with SAE. The configured action to be taken by SAE is \$configuredAction.:RAISE <p>When the trap is cleared, the text displayed is:</p> <ul style="list-style-type: none"> INFORMATION:SAE Router Driver: The configured state of router \$juniSaeRouterClientId is successfully resynchronized with SAE.:CLEAR
agentStarted	110	INFORMATION:Agent: The agent has started.:RAISE

Table 23: Event Traps (continued)

Trap Event	Trap ID	Text Displayed
agentRestartFailed	111	CRITICAL: Agent: The agent has failed to restart after \$ATTEMPTS attempts:RAISE
agentShutdown	112	INFORMATION:Agent:The agent has shutdown.:RAISE
componentUp	114	INFORMATION:\$I: This component is up.:RAISE
componentDown	115	INFORMATION:\$I: This component is down:RAISE
dirConnected	130	INFORMATION:\$I:The directory connection has been established with \$LDAP_HOST on port \$LDAP_PORT, and has a type of \$CONNECTION_TYPE.:RAISE
dirConnectionFailure	131	CRITICAL:\$I:The directory connection with \$LDAP_HOST has failed.:RAISE
dirNotAvail	132	CRITICAL:\$I:A directory connection is not available.:RAISE
nicHostRedundStateSwitched	240	INFORMATION:NIC Host: The redundancy state of the NIC Host has switched to \$juniNicHostRedundState.:RAISE
nicHostMisconfigured	241	INFORMATION:NIC Host: The NIC Host failed to start due to misconfiguration. The error message is "\$MESSAGE".:RAISE
nicHostBlacklistedSAE	242	CRITICAL:NIC sae-client agent:Blacklisted SAE: <SAE-KEY>.:RAISE
acpSyncCompleted	290	INFORMATION: ACP State Sync:ACP finished state sync with SAE for \$juniAcpVirtualRouterName.:RAISE
acpRedundStateSwitched	291	INFORMATION: ACP Host:The redundancy state of the ACP Host has switched to \$juniAcpRedundState.:RAISE
acpCPUUsage	281	<p>When the trap is raised, the text displayed is:</p> <ul style="list-style-type: none"> 'CRITICAL:ACP:{acpCPUUsed%}% of congestion point is in use. This exceeded the threshold of {THRESHOLD}%.:RAISE' where acpCPUUsed% is the percentage of bandwidth in use out of the total bandwidth of the congestion point. 'MAJOR:ACP:{acpCPUUsed%}% of congestion point is in use. This is below the threshold of {THRESHOLD}%.:RAISE' where acpCPUUsed% is the percentage of bandwidth in use out of the total bandwidth of the congestion point. 'MINOR:ACP:{acpCPUUsed%}% of congestion point is in use. This exceeded the threshold of {THRESHOLD}%.:RAISE' where acpCPUUsed% is the percentage of bandwidth in use out of the total bandwidth of the congestion point. <p>When the trap is cleared, the text displayed is:</p> <ul style="list-style-type: none"> 'CLEAR:ACP:{acpCPUUsed%}% of congestion point is in use. This is below the threshold of {THRESHOLD}%.:CLEAR' where acpCPUUsed% is the percentage of bandwidth in use out of the total bandwidth of the congestion point.
jpsAmConnUp	260	INFORMATION: JPS:A new application manager connection was established.:RAISE
jpsAmConnDown	261	INFORMATION:JPS:The application manager connection went down.:RAISE

Table 23: Event Traps (continued)

Trap Event	Trap ID	Text Displayed
jpsCmtsConnUp	262	INFORMATION:JPS:A new CMTS connection was established.:RAISE
jpsCmtsConnDown	263	INFORMATION:JPS:A CMTS connection went down.:RAISE
jdbReplicationFailure	292	<p>When the trap is raised, the text displayed is:</p> <ul style="list-style-type: none"> INFORMATION:jdbReplicationFailure:Failed to replicate LDAP data {juniSdxJdbReplicationDirection} neighbor {juniSdxJdbNeighbor}.The latest JDB replicaion status is:{juniSdxJdbLastStatus }:RAISE <p>When the trap is cleared, the text displayed is:</p> <ul style="list-style-type: none"> INFORMATION: jdbReplicationFailure:Community directory server {juniSdxJdbNeighbor} latest update status error:CLEAR
systemOperatingFailure	300	<p>When the trap is raised, the text displayed is:</p> <ul style="list-style-type: none"> INFORMATION:System:hardware failure is found with \$juniSdxOperatingSensor on system \$juniSdxOperatingLocation:RAISE <p>When the trap is cleared, the text displayed is:</p> <ul style="list-style-type: none"> INFORMATION:System:hardware failure with \$juniSdxOperatingSensor on system \$juniSdxOperatingLocation is cleared:CLEAR
diskFailure	301	<p>When the trap is raised, the text displayed is:</p> <ul style="list-style-type: none"> INFORMATION:System:disk failure is found:RAISE <p>When the trap is cleared, text displayed is:</p> <ul style="list-style-type: none"> INFORMATION:System:disk failure is cleared:CLEAR

- Related Documentation**
- [SNMP Traps Overview on page 83](#)
 - [Configuring Event Traps \(SRC CLI\) on page 87](#)
 - [Alarm State Transitions on page 106](#)

Alarm State Transitions

Table 24 on page 106 lists the alarm state transitions.

Table 24: Alarm State Transitions

Last Data Threshold	Current Data Threshold	Action(s)
NONE	NONE	No action
NONE	MINOR	Raise minor event

Table 24: Alarm State Transitions (continued)

Last Data Threshold	Current Data Threshold	Action(s)	
NONE	MAJOR	Raise major event	
NONE	CRITICAL	Raise critical event	
MINOR	NONE	Clear minor event	
MINOR	MINOR	No action	
MINOR	MAJOR	Raise major event	
MINOR	CRITICAL	Raise critical event	
MAJOR	NONE	Clear critical event	
MAJOR	MINOR	Clear major event	Raise minor event
MAJOR	MAJOR	No action	
MAJOR	CRITICAL	Raise critical event	
CRITICAL	NONE	Clear critical event	
CRITICAL	MINOR	Clear critical event	Raise minor event
CRITICAL	MAJOR	Clear critical event	Raise major event
CRITICAL	CRITICAL	No action	

- Related Documentation**
- [Configuring Event Traps \(SRC CLI\) on page 87](#)
 - [Event Traps on page 103](#)

PART 5

Monitoring the SRC Software and the C Series Controller with the C-Web Interface and the SRC CLI

- [Monitoring with the SRC CLI and the C-Web Interface on page 111](#)
- [Monitoring the System \(SRC CLI\) on page 115](#)
- [Monitoring the System \(C-Web Interface\) on page 123](#)
- [Monitoring SAE Data \(SRC CLI\) on page 133](#)
- [Monitoring SAE Data \(C-Web Interface\) on page 169](#)
- [Monitoring and Troubleshooting the NIC \(SRC CLI\) on page 195](#)
- [Monitoring the NIC \(C-Web Interface\) on page 207](#)
- [Monitoring NTP \(SRC CLI\) on page 213](#)
- [Monitoring NTP \(C-Web Interface\) on page 217](#)
- [Monitoring Redirect Server \(SRC CLI\) on page 221](#)
- [Monitoring the Redirect Server and Filtered Traffic \(C-Web Interface\) on page 223](#)
- [Troubleshooting Network Connectivity \(SRC CLI\) on page 227](#)
- [Monitoring Network Connectivity \(C-Web Interface\) on page 233](#)
- [Monitoring Activity for SRC Components on page 235](#)

CHAPTER 12

Monitoring with the SRC CLI and the C-Web Interface

- [Monitoring with the SRC CLI and the C-Web Interface on page 111](#)
- [SRC Monitoring Options on page 111](#)

Monitoring with the SRC CLI and the C-Web Interface

You can use the **show** commands available with the SRC CLI to monitor the operation and configuration of your SRC environment.

The C-Web graphical user interface (GUI) allows you to monitor the operation and configuration of your SRC environment by using a Web browser with Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS) enabled.

Related Documentation

- [Monitoring and Troubleshooting Tools Overview on page 3](#)
- [SRC Monitoring Options on page 111](#)

SRC Monitoring Options

[Table 25 on page 112](#) lists and compares the monitoring options for the C-Web interface and the SRC CLI.

Table 25: Comparison of SRC Monitoring Options

C-Web Interface Monitor Option	Information Displayed	Corresponding SRC CLI Commands
ACP	Admission Control Plug-In (ACP) data and statistics	<ul style="list-style-type: none"> • show acp backbone congestion-point congestion-point-expression • show acp backbone congestion-point dn • show acp backbone service • show acp edge congestion-point dn • show acp edge congestion-point subscriber-session-id • show acp edge subscriber • show acp remote-update congestion-point dn • show acp remote-update congestion-point name • show acp remote-update subscriber • show acp statistics device • show acp statistics directory • show acp statistics general
CLI	SRC CLI level and authorization data	<ul style="list-style-type: none"> • show cli • show cli authorization
Component	Installed components	<ul style="list-style-type: none"> • show component
Date	System date and time	<ul style="list-style-type: none"> • show date
Disk	System disk status	<ul style="list-style-type: none"> • show disk status
Interfaces	System interfaces	<ul style="list-style-type: none"> • show interfaces
Iptables	Filtered traffic statistics from the iptables Linux tool	<ul style="list-style-type: none"> • show iptables
NIC	Network information collector (NIC) component configuration data and statistics, including NIC agents, resolvers, and process	<ul style="list-style-type: none"> • show nic data • show nic data agent • show nic data resolver • show nic statistics • show nic statistics agent • show nic statistics host • show nic statistics process • show nic statistics resolver • show nic slot number data • show nic slot number statistics
NTP	Network Time Protocol (NTP) configuration data and statistics	<ul style="list-style-type: none"> • show ntp associations • show ntp statistics • show ntp status

Table 25: Comparison of SRC Monitoring Options (continued)

C-Web Interface Monitor Option	Information Displayed	Corresponding SRC CLI Commands
Redirect server	Redirect server statistics	<ul style="list-style-type: none"> • show redirect server statistics
Route	Route data from the local system to a remote host	<ul style="list-style-type: none"> • show route
SAE	SAE configuration data and statistics	<ul style="list-style-type: none"> • show sae drivers • show sae interfaces • show sae licenses • show sae policies • show sae registered equipment • show sae registered login • show sae services • show sae statistics device • show sae statistics device common • show sae statistics directory • show sae statistics directory connections • show sae statistics license client • show sae statistics license device • show sae statistics license local • show sae statistics policy-management • show sae statistics process • show sae statistics radius • show sae statistics radius client • show sae statistics sessions • show sae subscribers • show sae subscribers accounting-user-id • show sae subscribers dn • show sae subscribers ip • show sae subscribers login-name • show sae subscribers service-name • show sae subscribers session-id • show sae threads
Security	Security certificate configuration and statistics	<ul style="list-style-type: none"> • show security certificate
System	SRC software and C Series Controller configuration data	<ul style="list-style-type: none"> • show configuration • show system boot-messages • show system information • show system ldap community • show system ldap server • show system ldap statistics • show system users

- Related Documentation**
- [Monitoring and Troubleshooting Tools Overview on page 3](#)
 - [Monitoring with the SRC CLI and the C-Web Interface on page 111](#)

CHAPTER 13

Monitoring the System (SRC CLI)

- Viewing Information About a C Series Controller (SRC CLI) on page 115
- Viewing Information About Components Installed (SRC CLI) on page 117
- Viewing Information About Boot Messages (SRC CLI) on page 118
- Viewing Information About Security Certificates (SRC CLI) on page 121

Viewing Information About a C Series Controller (SRC CLI)

Purpose View information about a C Series Controller.



.....

NOTE: When you issue the `show system information` command in a virtualized SRC software, the manufacturer, version, and serial number details are not displayed in the output. In addition, the product name is displayed as vSRC.

.....

Action user@host> show system information

System Identification

Hostname my-server
Manufacturer Juniper Networks
Product Name C-2000
Version 1.0
Serial Number 0207082006000001
UUID 48384441-5254-0030-4859-0030485977EE
Hostid e30a2e07
Software version SRC PE Release 7.0 [A.7.0.0-151]

System Time

Current time 2007-01-02 17:29:19 EST
Uptime 15 days, 1:07
Number of active users 3
Load Averages (1m/5m/15m) 0.23/0.22/0.14

Memory

Total 15G
Free 12G

CPU Info

Number of CPU Core(s) 4
CPU Model Dual Core AMD Opteron(tm) Processor 265
Clock Speed 1804.132 MHz

Disk Information

Mountpoint	Total	Used	Use%
/	2015M	956M	47%
/altroot	2015M	35M	1%
/altvar	29G	75M	0%
/boot	98M	14M	14%
/var	31G	216M	0%

Temperature

System 30.000 degrees C
Physical CPU-1 34.000 degrees C
Physical CPU-2 29.000 degrees C

```
Fan speed
Fan-1 9375 RPM
Fan-2 9375 RPM
```

For information about configuring C Series Controllers, see the *SRC PE C-Web Interface Configuration Guide*.

- Related Documentation**
- [Viewing Information About Boot Messages \(SRC CLI\) on page 118](#)
 - [Viewing Information About the System \(C-Web Interface\) on page 123](#)
 - [Viewing Information About Components Installed \(SRC CLI\) on page 117](#)
 - [Viewing Information About System Disk Status \(C-Web Interface\) on page 127](#)

Viewing Information About Components Installed (SRC CLI)

Purpose View release and status information for SRC components installed on a system.

Action user@host> show component

Installed Components			
Name	Version		Status
acp	Release: 7.8	Build: ACP.A.MAIN.1480	disabled
activity	Release: 7.8	Build: ACTIVITY.A.MAIN.1480	running
agent	Release: 7.8	Build: SYSMAN.A.MAIN.1480	disabled
appsvr	Release: 7.8	Build: JBOSS.A.MAIN.1480	disabled
cli	Release: MAIN	Build: CLI.A.MAIN.1480	running
diameter	Release: 7.8	Build: DIAMETER.A.MAIN.1480	running
dsa	Release: 7.8	Build: GATEWAYAPPS.A.MAIN.1480	disabled
editor	Release: 7.8	Build: EDITOR.A.MAIN.1480	running
extsubmon	Release: 7.8	Build: MONAGENT.A.MAIN.1480	disabled
gw-3gpp	Release: 7.8	Build: 3GPPGW.A.MAIN.1480	disabled
gy-3gpp	Release: 7.8	Build: 3GPPGY.A.MAIN.1480	running
ims	Release: 7.8	Build: IMS.A.MAIN.1480	disabled
jdb	Release: 7.8	Build: DIRXA.A.MAIN.1480	running
licSvr	Release: 7.8	Build: LICSVR.A.MAIN.1480	disabled
naming	Release: 7.8	Build: NAMING.A.MAIN.1480	running
nic	Release: 7.8	Build: GATEWAY.A.MAIN.1480	running
redir	Release: 7.8	Build: REDIR.A.MAIN.1480	disabled
sae	Release: 7.8	Build: SAE.A.MAIN.1480	running
sic	Release: 7.8	Build: SICCLI.A.MAIN.1480	disabled
vta	Release: 7.8	Build: VTA.A.MAIN.1480	disabled
webadm	Release: 7.8	Build: WEBADM.A.MAIN.1480	disabled

Meaning [Table 26 on page 118](#) describes the output fields for the **show component** command. Output fields are listed in the order in which they appear.

Table 26: Output Fields for show component

Field Name	Field Description
Name	Name of the component
Version	Version of the component
Status	State of the component, running or disabled

- Related Documentation**
- [Viewing Information About Components Installed \(C-Web Interface\) on page 125](#)
 - *Viewing C Series Controller Information*
 - *Directories on the C Series Controller*

Viewing Information About Boot Messages (SRC CLI)

Purpose If you encounter system problems in a C Series Controller after you start the system, you can view information about the boot process.

View messages generated during system boot.

Action user@host> show system boot-messages

```

Bootdata ok (command line is ro root=/dev/vg0/root console=tty0 console=ttyS0,96
00)
Linux version 2.6.9-42.0.3.ELsmp (buildcentos@x8664-build.centos.org) (gcc versi
on 3.4.6 20060404 (Red Hat 3.4.6-3)) #1 SMP Fri Oct 6 06:28:26 CDT 2006
BIOS-provided physical RAM map:
  BIOS-e820: 0000000000000000 - 000000000009ac00 (usable)
  BIOS-e820: 000000000009ac00 - 00000000000a0000 (reserved)
  BIOS-e820: 00000000000ea070 - 00000000000100000 (reserved)
  BIOS-e820: 00000000000100000 - 00000000dffc0000 (usable)
  BIOS-e820: 00000000dffc0000 - 00000000dffc0000 (ACPI data)
  BIOS-e820: 00000000dffc0000 - 00000000dfff0000 (ACPI NVS)
  BIOS-e820: 00000000dfff0000 - 00000000e0000000 (reserved)
  BIOS-e820: 00000000fec00000 - 00000000fec86000 (reserved)
  BIOS-e820: 00000000fee00000 - 00000000fee01000 (reserved)
  BIOS-e820: 00000000ffb00000 - 00000000100000000 (reserved)
  BIOS-e820: 00000000100000000 - 00000000220000000 (usable)
ACPI: RSDP (v000 ACPIAM ) @ 0x000000000000f7760
ACPI: RSDT (v001 A M I OEMRSDT 0x03000529 MSFT 0x00000097) @ 0x00000000dffc000
0
ACPI: FADT (v002 A M I OEMFACP 0x03000529 MSFT 0x00000097) @ 0x00000000dffc020
0
ACPI: MADT (v001 A M I OEMAPIC 0x03000529 MSFT 0x00000097) @ 0x00000000dffc039
0
ACPI: OEMB (v001 A M I AMI_OEM 0x03000529 MSFT 0x00000097) @ 0x00000000dffc040
0
ACPI: DSDT (v001 DVLG2 DVLG2007 0x00000007 INTL 0x02002026) @ 0x0000000000000000
0
No NUMA configuration found
Faking a node at 0000000000000000-0000000220000000
Bootmem setup node 0 0000000000000000-0000000220000000
No mptable found.
On node 0 totalpages: 2228224
  DMA zone: 4096 pages, LIFO batch:1
  Normal zone: 2224128 pages, LIFO batch:16
  HighMem zone: 0 pages, LIFO batch:1
DMI 2.3 present.
ACPI: PM-Timer IO Port: 0x408
ACPI: Local APIC address 0xfe00000
ACPI: LAPIC (acpi_id[0x01] lapic_id[0x00] enabled)
Processor #0 15:4 APIC version 16
ACPI: LAPIC (acpi_id[0x02] lapic_id[0x06] enabled)
Processor #6 15:4 APIC version 16
ACPI: LAPIC (acpi_id[0x03] lapic_id[0x01] enabled)
Processor #1 15:4 APIC version 16
ACPI: LAPIC (acpi_id[0x04] lapic_id[0x07] enabled)
Processor #7 15:4 APIC version 16
Setting APIC routing to flat
ACPI: IOAPIC (id[0x08] address[0xfec00000] gsi_base[0])
IOAPIC[0]: apic_id 8, version 32, address 0xfec00000, GSI 0-23
ACPI: IOAPIC (id[0x09] address[0xfec10000] gsi_base[24])
IOAPIC[1]: apic_id 9, version 32, address 0xfec10000, GSI 24-4
ACPI: INT_SRC_OVR (bus 0 bus_irq 0 global_irq 2 dfl dfl)
ACPI: INT_SRC_OVR (bus 0 bus_irq 9 global_irq 9 high level)
ACPI: IRQ0 used by override.
ACPI: IRQ2 used by override.
ACPI: IRQ9 used by override.
Using ACPI (MADT) for SMP configuration information

```

```

Allocating PCI resources starting at e2000000 (gap: e0000000:1ec00000)
Checking aperture...
Built 1 zonelists
Kernel command line: ro root=/dev/vg0/root console=tty0 console=ttyS0,9600
Initializing CPU#0
PID hash table entries: 4096 (order: 12, 131072 bytes)
time.c: Using 3.579545 MHz PM timer.
time.c: Detected 3200.267 MHz processor.
Console: colour VGA+ 80x25
Dentry cache hash table entries: 2097152 (order: 12, 16777216 bytes)
Inode-cache hash table entries: 1048576 (order: 11, 8388608 bytes)
Placing software IO TLB between 0x28c1000 - 0x68c1000
Memory: 8168568k/8912896k available (2106k kernel code, 0k reserved, 1297k data,
196k init)
Calibrating delay using timer specific routine.. 6406.43 BogoMIPS (1pj=3203218)
Security Scaffold v1.0.0 initialized
SELinux: Initializing.
SELinux: Starting in permissive mode
There is already a security framework initialized, register_security failed.
selinux_register_security: Registering secondary module capability
Capability LSM initialized as secondary
Mount-cache hash table entries: 256 (order: 0, 4096 bytes)
CPU: Trace cache: 12K uops, L1 D cache: 16K
CPU: L2 cache: 2048K
using mwait in idle threads.
CPU0: Initial APIC ID: 0, Physical Processor ID: 0
Using IO APIC NMI watchdog
CPU: Trace cache: 12K uops, L1 D cache: 16K
CPU: L2 cache: 2048K
CPU0: Initial APIC ID: 0, Physical Processor ID: 0
CPU0: Intel(R) Xeon(TM) CPU 3.20GHz stepping 03
per-CPU timeslice cutoff: 705.82 usecs.
task migration cache decay timeout: 1 msecs.
Booting processor 1/6 rip 6000 rsp 10006945f58
Initializing CPU#1
Calibrating delay using timer specific routine.. 6399.38 BogoMIPS (1pj=3199690)
CPU: Trace cache: 12K uops, L1 D cache: 16K
CPU: L2 cache: 2048K
CPU1: Initial APIC ID: 6, Physical Processor ID: 3
Intel(R) Xeon(TM) CPU 3.20GHz stepping 03
Booting processor 2/1 rip 6000 rsp 1000697df58
Initializing CPU#2
Calibrating delay using timer specific routine.. 6399.32 BogoMIPS (1pj=3199664)
CPU: Trace cache: 12K uops, L1 D cache: 16K
CPU: L2 cache: 2048K

```

For information about configuring C Series Controllers, see the *SRC PE C-Web Interface Configuration Guide*.

Related Documentation

- [Viewing Information About Boot Messages \(C-Web Interface\) on page 126](#)
- [Viewing Information About a C Series Controller \(SRC CLI\) on page 115](#)
- [Viewing Information About Components Installed \(SRC CLI\) on page 117](#)

- [Viewing Information About System Disk Status \(C-Web Interface\) on page 127](#)

Viewing Information About Security Certificates (SRC CLI)

Purpose View information about security certificates that reside on the system.

Action user@host> show security certificate

```
web subject:CN=myhost
CAcert1 subject:CN=myhost
```

Meaning If no security certificates reside on the system, the CLI return a message to that effect:

```
user@host> show security certificate
No entity certificates in key store
```

For information about managing security digital certificates, see *Digital Certificates Overview*.

Related Documentation • [Viewing Information About Security Certificates \(C-Web Interface\) on page 126](#)

CHAPTER 14

Monitoring the System (C-Web Interface)

- [Viewing Information About the System \(C-Web Interface\) on page 123](#)
- [Viewing the System Date and Time \(C-Web Interface\) on page 124](#)
- [Viewing Information About Components Installed \(C-Web Interface\) on page 125](#)
- [Viewing Information About Boot Messages \(C-Web Interface\) on page 126](#)
- [Viewing Information About Security Certificates \(C-Web Interface\) on page 126](#)
- [Viewing Information About System Disk Status \(C-Web Interface\) on page 127](#)
- [Viewing Information About the Users on the System \(C-Web Interface\) on page 128](#)
- [Viewing Information About the Juniper Networks Database in Community Mode \(C-Web Interface\) on page 129](#)
- [Viewing Statistics for the Juniper Networks Database \(C-Web Interface\) on page 129](#)
- [Viewing Information About the SRC CLI \(C-Web Interface\) on page 130](#)

Viewing Information About the System (C-Web Interface)

Purpose View system information.

You can view information about the SRC software, including system identification and the system time. You can also view information about the environment of the C Series Controller, including memory, temperature, and fan speeds.

Action • Click **Monitor>System>Information**.

The Information pane displays the system information.

Figure 1: C-Web Interface for Monitoring System Information

System Identification	
Hostname	gaspode
Manufacturer	Juniper Networks
Product Name	SDX-2000
Version	1.0
Serial Number	0207082006000003
UUID	48384441-5254-0030-4859-003048595D02
Hostid	e30a2f07
Software version	SDX-300 Release . [A.MAIN-110] (January 22, 2007 02:20)

System Time	
Current time	2007-08-24 14:07:16 EDT
Uptime	76 days, 18:35
Number of active users	3
Load Averages (1m/5m/15m)	0.27/0.06/0.02

Memory	
Total	15G
Free	13G

CPU Info	
Number of CPU	4
CPU Model	Dual Core AMD Opteron(tm) Processor 265

For information about configuring C Series Controllers, see the *SRC PE C-Web Interface Configuration Guide*.

- Related Documentation**
- [Viewing Information About a C Series Controller \(SRC CLI\) on page 115](#)
 - [Viewing Information About Boot Messages \(C-Web Interface\) on page 126](#)
 - [Viewing Information About System Disk Status \(C-Web Interface\) on page 127](#)

Viewing the System Date and Time (C-Web Interface)

Purpose View the system date and time.

Action Click **Monitor>Date**.

The Date pane displays the date and time of the system.

Figure 2: C-Web Interface for Monitoring System Date and Time



Related Documentation

- [Setting the Time Zone \(SRC CLI\)](#)
- [Setting the System Date \(SRC CLI\)](#)
- [Viewing NTP Peers \(C-Web Interface\) on page 217](#)
- [Viewing Statistics for NTP \(C-Web Interface\) on page 218](#)
- [Viewing NTP Status \(C-Web Interface\) on page 218](#)

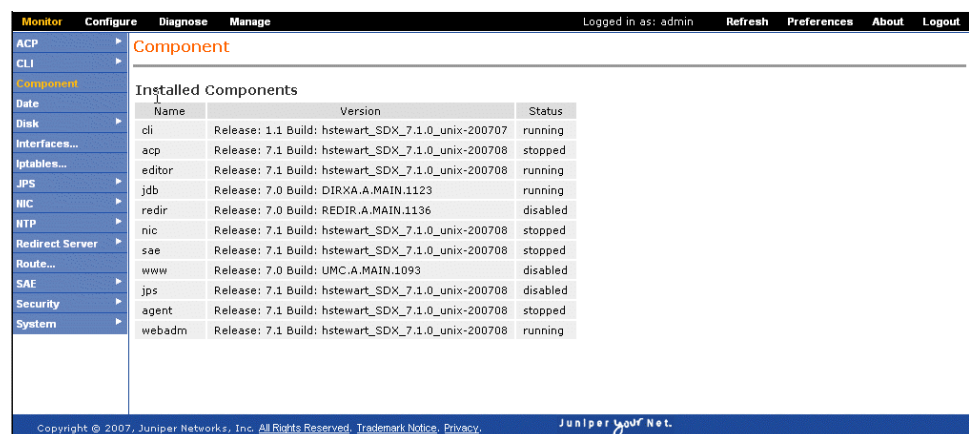
Viewing Information About Components Installed (C-Web Interface)

Purpose View the installed SRC components.

Action Click **Monitor>Component**.

The Component pane displays the status of each installed component.

Figure 3: C-Web Interface for Monitoring SRC Components Status



- Related Documentation**
- [Viewing Information About Components Installed \(SRC CLI\) on page 117](#)
 - [Viewing C Series Controller Information](#)
 - [Directories on the C Series Controller](#)

Viewing Information About Boot Messages (C-Web Interface)

Purpose View messages generated during SRC software startup.

Action Click **Monitor>System>Boot Messages**.

The Boot Messages pane displays the boot messages.

Figure 4: C-Web Interface for Monitoring System Boot Messages

Monitor		Logged in as: admin	About	Refresh	Logout
ACP	System				
CLI	Boot Messages				
Component					
Date	Fri Mar 9 10:17:24 EST 2007				
Disk	Feb 20 19:27:18 buffy genunix: [ID 936769 kern.info] dad0 is /pci@1f,0/ide@d/dad02,0				
Interfaces...	Feb 20 19:27:18 buffy dada: [ID 365891 kern.info] <ST360011A cyl 30307 alt 2 hd 16 sec 255>				
JPS	Feb 20 19:27:19 buffy swapgeneric: [ID 308332 kern.info] root on /pci@1f,0/ide@d/disk@2,0:a fstype ufs				
INC	Feb 20 19:27:19 buffy pcipsy: [ID 370704 kern.info] PCI-device: isa@7, ebus0				
NTF	Feb 20 19:27:19 buffy genunix: [ID 936769 kern.info] ebus0 is /pci@1f,0/isa@7				
Redirect Server	Feb 20 19:27:19 buffy ebus: [ID 521012 kern.info] su0 at ebus0: offset 0,3f8				
Route...	Feb 20 19:27:19 buffy genunix: [ID 936769 kern.info] su0 is /pci@1f,0/isa@7/serial@0,3f8				
SAE	Feb 20 19:27:19 buffy ebus: [ID 521012 kern.info] sul at ebus0: offset 0,2e8				
Security	Feb 20 19:27:19 buffy genunix: [ID 936769 kern.info] sul is /pci@1f,0/isa@7/serial@0,2e8				
System	Feb 20 19:27:19 buffy unix: [ID 987524 kern.info] cpu0: SUNW,UltraSPARC-IIe (upaid 0 impl 0x13 ver 0x33 clock 548 MHz)				
	Feb 20 19:27:20 buffy pcipsy: [ID 370704 kern.info] PCI-device: usb@a, ohci0				
	Feb 20 19:27:20 buffy genunix: [ID 936769 kern.info] ohci0 is /pci@1f,0/usb@a				
	Feb 20 19:27:22 buffy gld: [ID 944156 kern.info] dmfel0: Davicom DM9102 (v1.1): type "ether" mac address 00:03:ba:ce:d7:79				
	Feb 20 19:27:22 buffy pcipsy: [ID 370704 kern.info] PCI-device: ethernet@5, dmfel0				
	Feb 20 19:27:22 buffy genunix: [ID 936769 kern.info] dmfel0 is /pci@1f,0/ethernet@5				
	Feb 20 19:27:23 buffy gld: [ID 944156 kern.info] dmfel: Davicom DM9102 (v1.1): type "ether" mac address 00:03:ba:ce:d7:7a				
	Feb 20 19:27:22 buffy pcipsy: [ID 370704 kern.info] PCI-device: ethernet@5, dmfel				
	Feb 20 19:27:22 buffy genunix: [ID 936769 kern.info] dmfel is /pci@1f,0/ethernet@5				
	Feb 20 19:27:23 buffy genunix: [ID 454863 kern.info] dump on /dev/dsk/c0t2d0s1 size 2000 MB				
	Feb 20 19:27:24 buffy dmfel: [ID 426308 kern.info] dmfel0: PHY 1 link up 100 Mbps Full-Duplex				
	Feb 20 19:27:24 buffy date: [ID 247903 kern.notice] NOTICE: dmfel: PHY 1 link down				
	Feb 20 19:27:25 buffy pseudo: [ID 129642 kern.info] pseudo-device: devinfo0				
	Feb 20 19:27:25 buffy genunix: [ID 936769 kern.info] devinfo0 is /pseudo/devinfo@0				
	Feb 20 19:27:26 buffy scsi: [ID 193665 kern.info] sd0 at uata0: target 3 lun 0				
	Feb 20 19:27:26 buffy genunix: [ID 936769 kern.info] sd0 is /pci@1f,0/ide@d/sd@3,0				
	Feb 20 19:27:26 buffy ebus: [ID 521012 kern.info] isadma0 at ebus0: offset 0,0				
	Feb 20 19:27:26 buffy pseudo: [ID 129642 kern.info] pseudo-device: fssnap0				
	Feb 20 19:27:26 buffy genunix: [ID 936769 kern.info] fssnap0 is /pseudo/fssnap@0				
	Feb 20 19:27:26 buffy pseudo: [ID 129642 kern.info] pseudo-device: winlock0				
	Feb 20 19:27:26 buffy genunix: [ID 936769 kern.info] winlock0 is /pseudo/winlock@0				
	Feb 20 19:27:27 buffy pseudo: [ID 129642 kern.info] pseudo-device: lockstat0				

- Related Documentation**
- [Viewing Information About a C Series Controller \(SRC CLI\) on page 115](#)
 - [Viewing Information About Boot Messages \(SRC CLI\) on page 118](#)
 - [Viewing Information About the System \(C-Web Interface\) on page 123](#)
 - [Viewing Information About System Disk Status \(C-Web Interface\) on page 127](#)

Viewing Information About Security Certificates (C-Web Interface)

Purpose View messages generated during SRC software startup.

Action 1. Click **Monitor>Security>Certificate**.

The Certificate pane appears.

Figure 5: C-Web Interface for Monitoring Security Certificates



2. To display authority certificates, select the **Trusted** check box.

3. Click **OK**.

The Certificate pane displays the security certificates.

For information about managing security digital certificates, see *Digital Certificates Overview*.

Related Documentation

- [Viewing Information About Security Certificates \(SRC CLI\) on page 121](#)

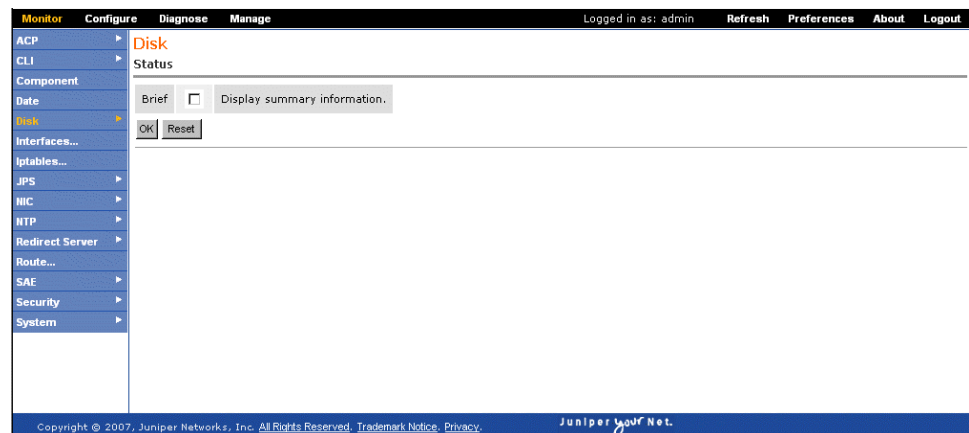
Viewing Information About System Disk Status (C-Web Interface)

Purpose View information about the system disk status.

Action 1. Click **Monitor>Disk>Status**.

The Status pane appears.

Figure 6: C-Web Interface for Monitoring System Disk Status



2. To display a summary of the system disk status, select the **Brief** check box.
3. Click **OK**.

The Status pane displays the system disk status.

Related Documentation

- [Viewing Information About a C Series Controller \(SRC CLI\) on page 115](#)
- [Viewing Information About the System \(C-Web Interface\) on page 123](#)
- [Viewing Information About Boot Messages \(C-Web Interface\) on page 126](#)

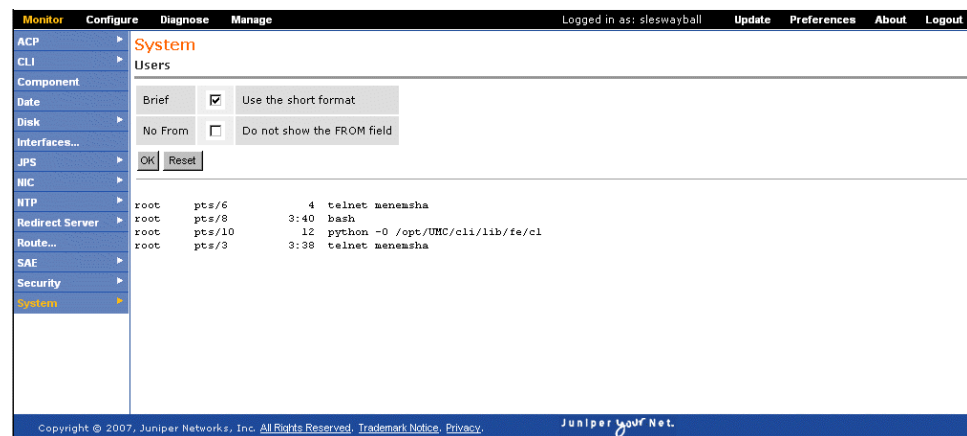
Viewing Information About the Users on the System (C-Web Interface)

Purpose View information about the users on the system.

- Action** 1. Click **Monitor>System>Users**.

The Users pane appears.

Figure 7: C-Web Interface for Monitoring System Users



2. To display a summary of the users, select the **Brief** check box.
3. Click **OK**.

The Users pane displays the information about the users on the system.

Related Documentation

- [Configuring User Accounts \(C-Web Interface\)](#)
- [Viewing Information About the SRC CLI \(C-Web Interface\) on page 130](#)
- [Viewing Information About SRC CLI User Permissions \(C-Web Interface\) on page 131](#)

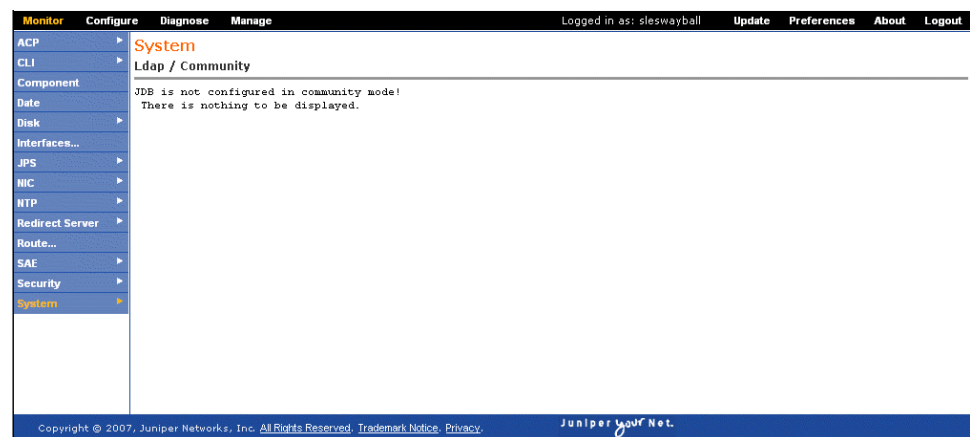
Viewing Information About the Juniper Networks Database in Community Mode (C-Web Interface)

Purpose View information about the Juniper Networks database when it runs in community mode.

Action Click **Monitor>System>LDAP>Community**.

The LDAP/Community pane appears and displays information about the Juniper Networks database.

Figure 8: C-Web Interface for Monitoring Juniper Networks Database in Community Mode



- Related Documentation**
- [Configuring the Juniper Networks Database to Run in Community Mode \(C-Web Interface\)](#)
 - [Viewing Statistics for the Juniper Networks Database \(C-Web Interface\)](#) on page 129

Viewing Statistics for the Juniper Networks Database (C-Web Interface)

Purpose View statistics for the Juniper Networks database.

Action Click **Monitor>System>LDAP>Statistics**.

The Statistics pane appears and displays local Juniper Networks database statistics.

Figure 9: C-Web Interface for Monitoring Local Juniper Networks Database Statistics

Monitor	Configure	Diagnose	Manage	Logged in as: sleswayball	Update	Preferences	About	Logout
ACP		System						
CLI		Ldap / Statistics						
Component								
Date		Local JDB statistics						
Disk		Number of Add operations since startup	993					
Interfaces...		Number of Delete operations since startup	0					
JPS		Number of Modify operations since startup	282					
NIC		Number of Rename operations since startup	0					
NTP		Number of Read operations since startup	480933					
Redirect Server		Number of List operations since startup	93821					
Route...		Number of Subtree Search operations since startup	367916					
SAE		Number of Bind operations	18266					
Security		Number of Anonymous Bind operations since startup	18232					
Speltem		Number of Compare operations since startup	0					
		Number of current connections	19					
		Number of all connections since startup	18266					
		Number of bind errors since startup	0					
		Number of all errors since startup	226721					
Copyright © 2007, Juniper Networks, Inc. All Rights Reserved. Trademark Notice Privacy Juniper Your Net.								

- Related Documentation**
- [Troubleshooting Data Synchronization for Juniper Networks Databases \(SRC CLI\)](#)
 - [Viewing Information About the Juniper Networks Database in Community Mode \(C-Web Interface\) on page 129](#)

Viewing Information About the SRC CLI (C-Web Interface)

You can view information about the current user's permissions and editing level for the SRC CLI by:

- [Viewing Information About the SRC CLI \(C-Web Interface\) on page 130](#)
- [Viewing Information About SRC CLI User Permissions \(C-Web Interface\) on page 131](#)

Viewing Information About the SRC CLI (C-Web Interface)

Purpose View information about the current user's command completion setting and editing level for the SRC CLI.

Action Click **Monitor>CLI**.

The CLI pane appears and displays the information about the CLI.

Figure 10: C-Web Interface for Monitoring SRC CLI Settings



- See Also**
- [Creating an SRC Configuration](#)
 - [Starting the SRC CLI](#)
 - [Viewing Settings for the SRC CLI](#)
 - [Viewing Information About SRC CLI User Permissions \(C-Web Interface\)](#) on page 131

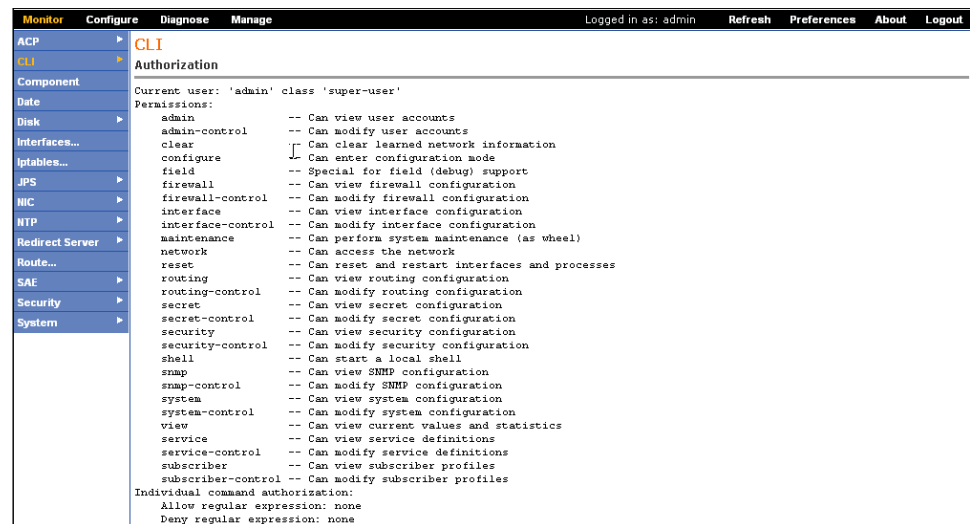
Viewing Information About SRC CLI User Permissions (C-Web Interface)

Purpose To display information about the current user's permissions for the SRC CLI.

Action Click **Monitor>CLI>Authorization**.

The Authorization pane appears and displays the current user's permissions for each SRC CLI option.

Figure 11: C-Web Interface for Monitoring SRC CLI User Permissions



- See Also**
- [Viewing Information About the SRC CLI \(C-Web Interface\) on page 130](#)
 - *Viewing Information about Users Logged Into the SRC Software*

CHAPTER 15

Monitoring SAE Data (SRC CLI)

- [Viewing SAE Data with the CLI on page 133](#)
- [Viewing Information About Subscriber Sessions \(SRC CLI\) on page 145](#)
- [Viewing SAE SNMP Information with the CLI on page 156](#)

Viewing SAE Data with the CLI

You can view information about the SAE active configuration for data currently stored in the SAE server's memory.

You can view SAE data by:

- [Viewing Information About the Directory Blacklist \(SRC CLI\) on page 133](#)
- [Viewing Information About SAE Device Drivers \(SRC CLI\) on page 134](#)
- [Viewing the Synchronization Status of SAE Session Stores \(SRC CLI\) on page 135](#)
- [Viewing Information About SAE Interfaces \(SRC CLI\) on page 136](#)
- [Viewing Information About SAE Licenses \(SRC CLI\) on page 137](#)
- [Viewing Information About Policies on the SAE \(SRC CLI\) on page 138](#)
- [Viewing Login Registrations \(SRC CLI\) on page 140](#)
- [Viewing Equipment Registrations \(SRC CLI\) on page 141](#)
- [Viewing Information About Services \(SRC CLI\) on page 141](#)
- [Viewing Information About Threads \(SRC CLI\) on page 144](#)

Viewing Information About the Directory Blacklist (SRC CLI)

Purpose View information about the directory blacklist configured on the SAE.

Action user@host> `show sae directory-black-list`

See Also

- *Removing the Directory Blacklist (C-Web Interface)*
- *Initially Configuring the SAE*

- [Viewing Information About the Directory Blacklist \(C-Web Interface\) on page 169](#)
- [Viewing Information About SAE Device Drivers \(SRC CLI\) on page 134](#)

Viewing Information About SAE Device Drivers (SRC CLI)

Purpose View information about SAE device drivers. Each device driver manages one logical router instance.

Action To view information about the state of SAE device drivers:

```
user@host> show sae drivers
```

```
JunosE Driver
Device name                default@dryad
Device type                junose
Device IP                  10.227.7.244
Local IP                   10.227.7.172
TransportRouter            default@dryad
Device version             7.2.0
Start time                 Tue Feb 13 14:18:44 EST 2007
Number of notifications    20
Number of processed added  14
Number of processed changed 0
Number of processed deleted 6
Number of provisioning attempt 30
Number of provisioning attempt failed 0
Number of outstanding decisions 0
Number of SAP              7
Number of PAP              1
Number of active user sessions 100
Number of active service sessions 0

  Job Queue
  Size                0
  Age (ms)            1
  Total enqueued      28
  Total dequeued      28
  Average job time (ms) 426
  State Synchronization
  Number recovered subscriber sessions 0
  Number recovered service sessions 0
  Number recovered interface sessions 0
  Number invalid subscriber sessions 0
  Number invalid service sessions 0
  Number invalid interface sessions 0
  Background restoration start time    Tue Feb 13 14:18:49 EST 2007

  Background restoration end time      Tue Feb 13 14:18:49 EST 2007

  Number subscriber sessions restored in background 0
  Number of provisioning objects left to collect 0
  Total number of provisioning objects to collect 11
  Start time                                   Tue Feb 13 14:18:45 EST 2007

  End time                                   Tue Feb 13 14:18:47 EST 2007

  Number of synched contexts 7
  Number of post-sync jobs 6
```

```

Session Store Info
Session Store Status          sessionsCollected
Status Last Update Time      Mon Jul 29 10:26:26 UTC 2013
Current Usage Ratio          1.0
Last Modified Time           Size(KB) Name LiveSessionsSize(KB)
Mon Jul 29 10:27:05 UTC 2013 117.9      storeOps_1_1 117.9

```

To view information about the state of a particular device driver, specify all or part of the virtual router name. For device drivers running Junos OS and PCMM drivers, use the format `default@routerName`.

```
user@host> show sae drivers device-name device-name
```

To view only the virtual router names for the device driver:

```
user@host> show sae drivers brief
```

```

Router Drivers
Router Name      Router Type
default@simJunos      junos

```

To restrict the number of displayed results:

```
user@host> show sae drivers maximum-results maximum-results
```

- See Also**
- [Initially Configuring the SAE](#)
 - [Shutting Down the Device Drivers \(SRC CLI\)](#)
 - [Viewing Information About Device Drivers \(C-Web Interface\) on page 172](#)
 - [Viewing Statistics for Device Drivers \(SRC CLI\) on page 163](#)

Viewing the Synchronization Status of SAE Session Stores (SRC CLI)

Purpose View the synchronization status of session stores. Session stores are used by SAE to store user session data and the service session data.

Action To view the SAE session stores synchronization status:

```
user@host> show sae sessionstore-stats
```

```

Session store Stats
Report Interval          300000 ms
Last Report Time         Thu Sep 12 10:54:12 UTC 2013
Operations Start Time    Thu Sep 12 10:54:12 UTC 2013
Number of Local Synchronizations 2

```

Time for All Local Synchronizations	106 ms
Bytes for All Local Synchronizations	0
Number of All Local Synchronized Files	2
Number of Community Synchronizations	2
Time for All Community Synchronizations	108 ms
Number of Remote Updates	0
Time for All Remote Updates	0 ms
Number of Operations	13
Time for All Operations	2 ms
Number of Rotations	0
Time for All Rotations	0 ms
Bytes for All Rotations	0
All Rotated Operations	0
Number of Snapshots	0
Time for All Snapshots	0 ms
Number of Keys for All Snapshots	0
Number of Flushes	3
Time for All Flushes	1 ms

- See Also**
- *Storing Subscriber and Service Session Data*
 - *Configuring the Session Store Feature (SRC CLI)*
 - [Viewing Information About SAE Device Drivers \(SRC CLI\) on page 134](#)

Viewing Information About SAE Interfaces (SRC CLI)

Purpose View information about SAE interfaces.

We recommend that you do not enter the **show sae interfaces** command without specifying an interface, virtual router, brief, or maximum results to filter the results. Entering the **show sae interfaces** command can generate a large quantity of results, and processing these results can place a load on the C Series Controller.

Action To view information about the router interfaces:

```
user@host> show sae interfaces
```

To view information about particular router interfaces, specify all or part of the interface name.

```
user@host> show sae interfaces interface-name interface-name
```

To view information about interfaces for a particular virtual router, specify all or part of the VR name.

```
user@host> show sae interfaces virtual-router-name virtual-router-name
```

To view only the interface names:

```
user@host> show sae interfaces brief
```

To restrict the number of displayed results:

```
user@host> show sae interfaces maximum-results maximum-results
```

- See Also**
- *Initially Configuring the SAE*
 - *Reloading Interface Classification Scripts (SRC CLI)*
 - [Viewing Information About Interfaces \(C-Web Interface\)](#) on page 174
 - [Viewing Information About SAE Device Drivers \(SRC CLI\)](#) on page 134

Viewing Information About SAE Licenses (SRC CLI)

Purpose View the installed licenses.

Action user@host> show sae licenses

```
SSC License Key Checker V3.0
```

```
Type of license: Server license. Connectivity to the specified SDX  
License server (Test): OK
```

```
The following valid licenses are found:
```

```
License: cn=@License,ou=licSvr,ou=Licenses,o=Management,o=UMC  
license.val.component = 3  
license.val.customer = jnpr  
license.val.expiry = 2020-12-12  
license.val.release = 7.*  
license.val.seqnum = 00002  
license.val.serialnum = 123  
license.val.server.corbaloc = corbaloc::SumanthTest:9000/licmanager  
license.val.serviceSessions = 90000  
license.val.type = server
```

See Also • *Obtaining an SRC License*

- [Viewing Information About Licenses \(C-Web Interface\)](#) on page 171
- [Viewing Information About Policies on the SAE \(SRC CLI\)](#) on page 138

Viewing Information About Policies on the SAE (SRC CLI)

Purpose View policy information.

Action To view information about the policies available on the SAE:

```
user@host> show sae policies
```

```
To view information about particular policies, specify all or part of the policy list name:
```

```
user@host> show sae policies filter filter
```


For example, if you wanted to view the policy called brickwall:

```
user@host> show sae policies filter brickwall
```

Policy Group

```
Policy Group Name brickwall
Absolute ID      policyGroupName=brickwall,ou=entjunos,o=Policies,o=UMC
```

Policy Object

```
applicability both
Name          both
policyRoles   Junos
accountingRule false
Name          block
priority      601
ruleType      Junos OS ASP
matchDirection both
Name          all
Name          drop
Name          packet
```

To view only the policy list names for the policies:

```
user@host> show sae policies brief
```

Policies

```
ADSL-Basic
basicBod
BestEffort64
block
bod
bodVpn
both_fwr_filter
both_fwr_fwd
both_fwr_reject
brickwall
brickwall
content-provider
content-provider-tiered
custom_policer
default
default
DHCP
DocsisParameter
DownStream
dynsrcnat
eglimit
emailweb
emailweb
EntDefault
filter
```

```
More results available. Display has reached the maximum number of results.  
Number of skipped results: 43
```

To restrict the number of displayed results:

```
user@host> show sae policies maximum-results maximum-results
```

- See Also**
- [Enabling the Policy Configuration on the SRC CLI](#)
 - [Viewing Information About Policies \(C-Web Interface\) on page 172](#)
 - [Viewing Information About SAE Licenses \(SRC CLI\) on page 137](#)
 - [Viewing SNMP Information for Policies \(SRC CLI\) on page 160](#)

Viewing Login Registrations (SRC CLI)

Purpose View information about registered logins. You can view all login registrations, or you can view a specific registration.

Action To view information about all login registrations:

```
user@host> show sae registered login
```

To view a specific registration, specify the media access control (MAC) address for the registration that you want to display:

```
user@host> show sae registered login mac-address mac-address
```

To view only the MAC address of the registrations:

```
user@host> show sae registered login brief
```

To restrict the number of displayed results:

```
user@host> show sae registered login maximum-results maximum-results
```

For information about login registrations, see the *SRC PE Sample Applications Guide*.

- See Also**
- [Removing Login Registrations \(SRC CLI\)](#)

- [Viewing Login Registrations \(C-Web Interface\) on page 176](#)

Viewing Equipment Registrations (SRC CLI)

Purpose View information about equipment registrations. You can view all equipment registrations, or you can view a specific registration.

Action To view information about all equipment registrations:

```
user@host> show sae registered equipment
```

To view a specific registration, specify the media access control (MAC) address for the registration that you want to display:

```
user@host> show sae registered equipment mac-address mac-address
```

To view only the MAC address of the registrations:

```
user@host> show sae registered equipment brief
```

To restrict the number of displayed results:

```
user@host> show sae registered equipment maximum-results maximum-results
```

For information about equipment registrations, see the *SRC PE Sample Applications Guide*.

- See Also**
- [Removing Equipment Registrations \(C-Web Interface\)](#)
 - [Viewing Equipment Registrations \(C-Web Interface\) on page 174](#)
 - [Viewing Login Registrations \(SRC CLI\) on page 140](#)

Viewing Information About Services (SRC CLI)

Purpose View information about services available on the SAE. You can view information about all services, or about specific services.

Action To view information about the services available on the SAE:

```
user@host> show sae services
```

To view information about particular services, specify all or part of the service name:

```
user@host> show sae services filter filter
```

For example, if you wanted to view the service called BrickWall:

```
user@host> show sae services filter brickwall
```

```
Service
available      true
description    This firewall blocks all incoming and outgoing traffic.
location       l=entjunos,o=scopes,o=umc
policygroupref policyGroupName=brickwall,ou=entjunos,o=Policies,o=UMC
servicename    BrickWall
servicetype    7
sspcategory    basicFirewall
ssptype        Normal
status         2
available      true
description    This firewall blocks all incoming and outgoing traffic.
location       l=entjunosstatelessfw,o=scopes,o=umc
policygroupref policyGroupName=brickwall,ou=entjunos_statelessfw,o=Policies,o=UMC
servicename    BrickWall
servicetype    7
sspcategory    basicFirewall
ssptype        Normal
status         2
```

To view all the hidden services:

```
user@host> show sae services secret
```

```
Service
available      true
description    This firewall blocks all incoming traffic and allows only
               outgoing email and web traffic.
location       l=entjunos,o=scopes,o=umc
policygroupref policyGroupName=emailweb,ou=entjunos,o=Policies,o=UMC
servicename    EmailAndWeb
servicetype    7
sspcategory    basicFirewall
sspradiusclass EmailAndWeb
ssptype        Normal
status         2
available      true
description    This firewall blocks all incoming traffic and allows only
               outgoing email and web traffic.
location       l=entjunosstatelessfw,o=scopes,o=umc
policygroupref policyGroupName=emailweb,ou=entjunos_statelessfw,o=Policies,o=UMC
servicename    EmailAndWeb
servicetype    7
sspcategory    basicFirewall
```

```

sspradiusclass EmailAndWeb
ssptype        Normal
status        2
Service
available      true
description    This service is activated automatically when the
               subscriber is the source or destination of a network
               attack
location       l=idp-subscriber,o=scopes,o=umc
parametersubstitution captiveAddress=66.13.2.11
policygroupref policyGroupName=quarantine,ou=idp,o=Policies,o=UMC
servicename    Quarantine
servicetype    7
sspradiusclass Quarantine
ssptype        Normal
status        2

```

To view only the service names for the services:

```
user@host> show sae services brief
```

```

Services
EmailAndWeb
Quarantine
Audio-Silver
Internet-Gold
Internet-Silver
DynSrcNat
FWR_Filter_Out
StaticDestNat
PingDoSProtect
MirrorFragment
SubrIntfFragment
BrickWall
Audio-Bronze
Internet-Bronze
Limit500kbs
News
Gold_VPN
Limit1Mbs
Video-Silver
Audio-Gold
RouterFragment
1.0 Mbps
DynSrcNat
FWR_Filter_Out
StaticDestNat
PingDoSProtect
MirrorFragment
SubrIntfFragment
BrickWall
Audio-Bronze
Internet-Bronze
Limit500kbs
News
Gold_VPN
Limit1Mbs
Video-Silver

```

```
Audio-Gold
RouterFragment
1.0 Mbps
FWR_Rej_In
MirrorAggregate
Video-Bronze
```

```
More results available. Display has reached the maximum number of results.
Number of skipped results: 26
```

To restrict the number of displayed results:

```
user@host> show sae services maximum-results maximum-results
```

- See Also**
- *Configuring Access to Service Data (SRC CLI)*
 - *Reloading Services (SRC CLI)*
 - [Viewing Information About Services \(C-Web Interface\)](#) on page 170

Viewing Information About Threads (SRC CLI)

Purpose View information about the threads and their priority on the SAE.

Action user@host> show sae threads

Thread Group

Thread group name system
 Active threads 112
 Active groups 11
 Max priority 10

Thread name	Priority	Daemon thread
Reference Handler	10	true
Finalizer	8	true
Signal Dispatcher	9	true

...

Thread Group

Thread group name RKSTrackingQueue
 Active threads 5
 Active groups 0
 Max priority 10

Thread name	Priority	Daemon thread
RKSTrackingQueue-0	5	true
RKSTrackingQueue-1	5	true
RKSTrackingQueue-2	5	true
RKSTrackingQueue-3	5	true
RKSTrackingQueue-4	5	true

See Also • [Viewing Information About Threads \(C-Web Interface\) on page 177](#)

Viewing Information About Subscriber Sessions (SRC CLI)

You can list subscriber sessions by:

- [Viewing General Information About Subscriber Sessions \(SRC CLI\) on page 146](#)
- [Viewing Information About Subscriber Sessions by DN \(SRC CLI\) on page 147](#)
- [Viewing Information About Subscriber Sessions by IP Address, VPN Identifier, or both \(SRC CLI\) on page 148](#)
- [Viewing Information About Subscriber Sessions by Login Name \(SRC CLI\) on page 150](#)
- [Viewing Information About Subscriber Sessions by Service Name \(SRC CLI\) on page 151](#)

- [Viewing Information About Subscriber Sessions by Session ID \(SRC CLI\) on page 152](#)
- [Viewing Information About Subscriber Sessions by Accounting User Identifier \(SRC CLI\) on page 154](#)
- [Viewing the Number of Active Service Sessions \(SRC CLI\) on page 155](#)
- [Viewing Subscriber Session Count Used by a Managed Router \(SRC CLI\) on page 155](#)

Viewing General Information About Subscriber Sessions (SRC CLI)

Purpose View general information about subscriber sessions. You can view all or restricted information about all subscriber sessions.

Action To view information about all subscriber sessions:

```
user@host> show sae subscribers
```

To view the subscriptions and service sessions from hidden services:

```
user@host> show sae subscribers secret
```

To view only the subscriber session information without service sessions:

```
user@host> show sae subscribers brief
```

```
user@host> show sae subscribers brief
User Session
User IPv4      192.167.0.0/32
User IPv6      2001:db8:85a3:0:0:8a2e:370:1c17/128
User DN        uniqueId=jane,ou=local,retailerName=default,o=Users,o=UMC
MAC Address    41:42:43:44:45:46
Device Name    default:vr0@simJunos
Login Name     jane1@virneo.net
Interface Name ip/192.167.0.0
RADIUS session ID wnNbqRW/b0/KMAPo
Login time     Thu May 11 10:15:27 UTC 2017
Session Timeout -1
Active Services [Internet-Bronze]
Available Services [News, Internet-Bronze]
user@host>
```

To view the subscriber session ID, login name, and IP address:

```
user@host> show sae subscribers terse
```

```
user@host> show sae subscribers terse
User Sessions
Session ID  Login Name      IPv4 Address      IPv6 Address
b0/KMAPo    jane1@virneo.net 192.167.0.0/32    2001:db8:85a3:0:0:8a2e:370:1c17/128
user@host>
```


To restrict the number of displayed results:

```
user@host> show sae subscribers maximum-results maximum-results
```

- See Also**
- [Configuring Access to Subscriber Data \(SRC CLI\)](#)
 - [Viewing Information About Subscriber Sessions by DN \(SRC CLI\) on page 147](#)
 - [Viewing Information About Subscriber Sessions by IP Address, VPN Identifier, or both \(SRC CLI\) on page 148](#)
 - [Viewing Information About Subscriber Sessions by Service Name \(SRC CLI\) on page 151](#)
 - [Viewing Information About Subscriber Sessions by Session ID \(SRC CLI\) on page 152](#)
 - [Viewing Information About Subscriber Sessions by Accounting User Identifier \(SRC CLI\) on page 154](#)

Viewing Information About Subscriber Sessions by DN (SRC CLI)

Purpose View information about subscriber sessions by the DN associated with the subscriber session. You can view all or restricted information about all associated subscriber sessions.

Action To view information about subscriber sessions accessible by DN:

```
user@host> show sae subscribers dn
```

To view information about specific subscriber sessions, use all or part of the DN:

```
user@host> show sae subscribers dn filter filter
```

To view information about subscriber sessions only by the exact match of the DN:

```
user@host> show sae subscribers dn filter filter exact
```



NOTE: You must configure the exact option along with the filter *filter* option, else all the subscriber sessions information accessible by DN is displayed.

To view the subscriptions and service sessions from hidden services:

```
user@host> show sae subscribers dn secret
user@host> show sae subscribers dn filter filter secret
```

To view only the subscriber session information without service sessions:

```
user@host> show sae subscribers dn brief
user@host> show sae subscribers dn filter filter brief
```

To view the subscriber session ID, login name, and IP address:

```
user@host> show sae subscribers dn terse
user@host> show sae subscribers dn filter filter terse
```

To restrict the number of displayed results:

```
user@host> show sae subscribers dn maximum-results maximum-results
user@host> show sae subscribers dn filter filter maximum-results maximum-results
```

- See Also**
- [Configuring Access to Subscriber Data \(SRC CLI\)](#)
 - [Viewing General Information About Subscriber Sessions \(SRC CLI\) on page 146](#)
 - [Viewing Information About Subscriber Sessions by IP Address, VPN Identifier, or both \(SRC CLI\) on page 148](#)
 - [Viewing Information About Subscriber Sessions by Service Name \(SRC CLI\) on page 151](#)
 - [Viewing Information About Subscriber Sessions by Session ID \(SRC CLI\) on page 152](#)
 - [Viewing Information About Subscriber Sessions by Accounting User Identifier \(SRC CLI\) on page 154](#)

Viewing Information About Subscriber Sessions by IP Address, VPN Identifier, or both (SRC CLI)

Purpose View information about subscriber sessions by the IP address, VPN identifier, or both associated with the subscriber session.

You can list subscriber sessions by IP address, VPN identifier, or both for Dynamic Host Configuration Protocol (DHCP) subscribers, authenticated Point-to-Point Protocol (PPP) subscribers, and static IP subscribers who have logged in to the portal.

Action To view information about subscriber sessions that are accessible by IP address:

```
user@host> show sae subscribers ip
```

To view information about a particular subscriber session that is accessible by IP address:

```
user@host> show sae subscribers ip address address
```

To view information about subscriber sessions only by the exact match of the IP address:

```
user@host> show sae subscribers ip address address exact
```



NOTE: You must configure the exact option along with the address *address* option, else the information about all the subscriber sessions that are accessible by IP address is displayed.

To view information about subscriber sessions that are accessible by VPN identifier:

```
user@host> show sae subscribers ip vpnid vpnid
```

To view information about a particular subscriber session that is accessible by both IP address and VPN identifier:

```
user@host> show sae subscribers ip address address vpnid vpnid
```

To view information about particular subscriber sessions, specify the IP address:

```
user@host> show sae subscribers ip filter filter
```

To view the subscriptions and service sessions from hidden services:

```
user@host> show sae subscribers ip secret
user@host> show sae subscribers ip filter filter secret
```

To view only the subscriber session information without service sessions:

```
user@host> show sae subscribers ip brief
user@host> show sae subscribers ip filter filter brief
```

To view the subscriber session ID, login name, and IP address:

```
user@host> show sae subscribers ip terse
user@host> show sae subscribers ip filter filter terse
```

To restrict the number of displayed results:

```
user@host> show sae subscribers ip maximum-results maximum-results
user@host> show sae subscribers ip filter filter maximum-results maximum-results
```

See Also • *Configuring Access to Subscriber Data (SRC CLI)*

- [Viewing General Information About Subscriber Sessions \(SRC CLI\) on page 146](#)
- [Viewing Information About Subscriber Sessions by DN \(SRC CLI\) on page 147](#)
- [Viewing Information About Subscriber Sessions by Service Name \(SRC CLI\) on page 151](#)
- [Viewing Information About Subscriber Sessions by Session ID \(SRC CLI\) on page 152](#)
- [Viewing Information About Subscriber Sessions by Accounting User Identifier \(SRC CLI\) on page 154](#)

Viewing Information About Subscriber Sessions by Login Name (SRC CLI)

Purpose View information about subscriber sessions by the subscriber login name. You can view all or restricted information about all associated subscriber sessions.

Action To view information about subscriber sessions accessible by login name:

```
user@host> show sae subscribers login-name
```

To view information about specific subscriber sessions, use all or part of the login name:

```
user@host> show sae subscribers login-name filter filter
```

To view information about subscriber sessions only by the exact match of the login name:

```
user@host> show sae subscribers login-name filter filter exact
```



NOTE: You must configure the exact option along with the filter *filter* option, else all the subscriber sessions information accessible by the subscriber login name is displayed.

To view the subscriptions and service sessions from hidden services:

```
user@host> show sae subscribers login-name secret
user@host> show sae subscribers login-name filter filter secret
```

To view only the subscriber session information without service sessions:

```
user@host> show sae subscribers login-name brief
user@host> show sae subscribers login-name filter filter brief
```

To view the subscriber session ID, login name, and IP address:

```
user@host> show sae subscribers login-name terse
```

```
user@host> show sae subscribers login-name filter filter terse
```

To restrict the number of displayed results:

```
user@host> show sae subscribers login-name maximum-results maximum-results
user@host> show sae subscribers login-name filter filter maximum-results maximum-results
```

- See Also**
- [Configuring Access to Subscriber Data \(SRC CLI\)](#)
 - [Viewing General Information About Subscriber Sessions \(SRC CLI\) on page 146](#)
 - [Viewing Information About Subscriber Sessions by DN \(SRC CLI\) on page 147](#)
 - [Viewing Information About Subscriber Sessions by IP Address, VPN Identifier, or both \(SRC CLI\) on page 148](#)
 - [Viewing Information About Subscriber Sessions by Session ID \(SRC CLI\) on page 152](#)
 - [Viewing Information About Subscriber Sessions by Accounting User Identifier \(SRC CLI\) on page 154](#)

Viewing Information About Subscriber Sessions by Service Name (SRC CLI)

Purpose View information about subscriber sessions that are associated with a specified service. You can view all or restricted information about all associated subscriber sessions.

Action To view information about subscriber sessions activated by a subscription to an active service session:

```
user@host> show sae subscribers service-name
```

To view information about specific subscriber sessions, use all or part of the service name:

```
user@host> show sae subscribers service-name filter filter
```

To view information about subscriber sessions only by the exact match of the service name:

```
user@host> show sae subscribers service-name filter filter exact
```



NOTE: You must configure the exact option along with the filter *filter* option, else information about all the subscriber sessions activated by a subscription to an active service session is displayed.

To view the subscriptions and service sessions from hidden services:

```
user@host> show sae subscribers service-name secret
user@host> show sae subscribers service-name filter filter secret
```

To view only the subscriber session information without service sessions:

```
user@host> show sae subscribers service-name brief
user@host> show sae subscribers service-name filter filter brief
```

To view the subscriber session ID, login name, and IP address:

```
user@host> show sae subscribers service-name terse
user@host> show sae subscribers service-name filter filter terse
```

To restrict the number of displayed results:

```
user@host> show sae subscribers service-name maximum-results maximum-results
user@host> show sae subscribers service-name filter filter maximum-results
maximum-results
```

- See Also**
- [Configuring Access to Subscriber Data \(SRC CLI\)](#)
 - [Viewing General Information About Subscriber Sessions \(SRC CLI\) on page 146](#)
 - [Viewing Information About Subscriber Sessions by DN \(SRC CLI\) on page 147](#)
 - [Viewing Information About Subscriber Sessions by IP Address, VPN Identifier, or both \(SRC CLI\) on page 148](#)
 - [Viewing Information About Subscriber Sessions by Session ID \(SRC CLI\) on page 152](#)

Viewing Information About Subscriber Sessions by Session ID (SRC CLI)

Purpose View information about subscriber sessions by the session ID associated with the subscriber session. You can view all or restricted information about all associated subscriber sessions.

Action To view information about subscriber sessions by session ID:

```
user@host> show sae subscribers session-id
```

To view information about specific subscriber sessions, use all or part of the subscriber session ID:

```
user@host> show sae subscribers session-id filter filter
```

To view information about subscriber sessions only by the exact match of the subscriber session ID:

```
user@host> show sae subscribers session-id filter filter exact
```



NOTE: You must configure the exact option along with the filter *filter* option, else all the subscriber sessions information by the session ID is displayed.

To view the subscriptions and service sessions from hidden services:

```
user@host> show sae subscribers session-id secret
user@host> show sae subscribers session-id filter filter secret
```

To view only the subscriber session information without service sessions:

```
user@host> show sae subscribers session-id brief
user@host> show sae subscribers session-id filter filter brief
```

To view the subscriber session ID, login name, and IP address:

```
user@host> show sae subscribers session-id terse
user@host> show sae subscribers session-id filter filter terse
```

To restrict the number of displayed results:

```
user@host> show sae subscribers session-id maximum-results maximum-results
user@host> show sae subscribers session-id filter filter maximum-results maximum-results
```

- See Also**
- [Configuring Access to Subscriber Data \(SRC CLI\)](#)
 - [Viewing General Information About Subscriber Sessions \(SRC CLI\) on page 146](#)
 - [Viewing Information About Subscriber Sessions by DN \(SRC CLI\) on page 147](#)
 - [Viewing Information About Subscriber Sessions by IP Address, VPN Identifier, or both \(SRC CLI\) on page 148](#)
 - [Viewing Information About Subscriber Sessions by Service Name \(SRC CLI\) on page 151](#)

- [Viewing Information About Subscriber Sessions by Accounting User Identifier \(SRC CLI\)](#) on page 154

Viewing Information About Subscriber Sessions by Accounting User Identifier (SRC CLI)

Purpose View information about subscriber sessions by the accounting user identifier associated with the subscriber session. You can view all or specific information about all associated subscriber sessions.

Action To view information about subscriber sessions accessible by accounting user identifier:

```
user@host> show sae subscribers accounting-user-id
```

To view information about specific subscriber sessions, use all or part of the accounting user identifier:

```
user@host> show sae subscribers accounting-user-id filter filter
```

To view information about subscriber sessions only by the exact match of accounting user identifier:

```
user@host> show sae subscribers accounting-user-id filter filter exact
```



NOTE: You must configure the exact option along with the filter *filter* option, else the information about all the subscriber sessions accessible by the accounting user identifier is displayed.

To view the subscriptions and service sessions from hidden services:

```
user@host> show sae subscribers accounting-user-id secret  
user@host> show sae subscribers accounting-user-id filter filter secret
```

To view only the subscriber session information without service sessions:

```
user@host> show sae subscribers accounting-user-id brief  
user@host> show sae subscribers accounting-user-id filter filter brief
```

To view the subscriber session ID, login name, and IP address:

```
user@host> show sae subscribers accounting-user-id terse  
user@host> show sae subscribers accounting-user-id filter filter terse
```

To restrict the number of displayed results:

```
user@host> show sae subscribers accounting-user-id maximum-results maximum-results
```



```
user@host> show sae subscribers accounting-user-id filter filter maximum-results
maximum-results
```

- See Also**
- [Viewing General Information About Subscriber Sessions \(SRC CLI\) on page 146](#)
 - [Viewing Information About Subscriber Sessions by Login Name \(SRC CLI\) on page 150](#)
 - [Viewing Information About Subscriber Sessions by DN \(SRC CLI\) on page 147](#)
 - [Viewing Information About Subscriber Sessions by IP Address, VPN Identifier, or both \(SRC CLI\) on page 148](#)
 - [Viewing Information About Subscriber Sessions by Session ID \(SRC CLI\) on page 152](#)

Viewing the Number of Active Service Sessions (SRC CLI)

Purpose View the number of currently active service sessions that exist for a given service, service attribute, scope, and virtual router.

Action To view the number of currently active service sessions for a given service, service attribute, scope, and virtual router:

```
user@host> show sae number-service-sessions service-name service-name service-attribute-name
service-attribute-name scope scope virtual-router virtual-router
```

- See Also**
- [Configuring Access to Subscriber Data \(SRC CLI\)](#)
 - [Viewing General Information About Subscriber Sessions \(SRC CLI\) on page 146](#)
 - [Viewing Information About Subscriber Sessions by DN \(SRC CLI\) on page 147](#)
 - [Viewing Information About Subscriber Sessions by IP Address, VPN Identifier, or both \(SRC CLI\) on page 148](#)
 - [Viewing Information About Subscriber Sessions by Service Name \(SRC CLI\) on page 151](#)

Viewing Subscriber Session Count Used by a Managed Router (SRC CLI)

Purpose View the number of subscriber sessions used by a managed router. This command displays the number of subscriber sessions used for both managed and unmanaged subscribers. (Unmanaged subscribers are users who do not have volume-based billing.) It also displays the device used for the router or virtual router.

Action To view the number of subscriber sessions used by a managed router:

```
user@host> show sae statistics device name name terse
user@host> show sae statistics device name default@jrouter terse
SNMP Statistics
Device Name          Device      Type      Managed Interfaces  Unmanaged
```

```
Interfaces
default@test      JunosE      COPS        1              8
user@host>
```

- See Also**
- [Configuring Access to Subscriber Data \(SRC CLI\)](#)
 - [Viewing General Information About Subscriber Sessions \(SRC CLI\) on page 146](#)
 - [Viewing Information About Subscriber Sessions by DN \(SRC CLI\) on page 147](#)
 - [Viewing Information About Subscriber Sessions by IP Address, VPN Identifier, or both \(SRC CLI\) on page 148](#)
 - [Viewing Information About Subscriber Sessions by Service Name \(SRC CLI\) on page 151](#)

Viewing SAE SNMP Information with the CLI

You can view state information that is also available through SNMP, including information about counters that describe the SAE history of activity. This information is the same as the information you can view from the SAE SNMP interface. You can monitor SNMP by:

- [Viewing Statistics About the Directory \(SRC CLI\) on page 156](#)
- [Viewing Statistics for Directory Connections \(SRC CLI\) on page 157](#)
- [Viewing SNMP Information for Client Licenses \(SRC CLI\) on page 159](#)
- [Viewing SNMP Information for Local Licenses \(SRC CLI\) on page 159](#)
- [Viewing SNMP Information for Licenses on Virtual Routers \(SRC CLI\) on page 160](#)
- [Viewing SNMP Information for Policies \(SRC CLI\) on page 160](#)
- [Viewing SNMP Information for the SAE Server Process \(SRC CLI\) on page 161](#)
- [Viewing Statistics for RADIUS Clients \(SRC CLI\) on page 161](#)
- [Viewing SNMP Information for RADIUS Clients \(SRC CLI\) on page 162](#)
- [Viewing SNMP Information for Routers and Devices \(SRC CLI\) on page 163](#)
- [Viewing Statistics for Device Drivers \(SRC CLI\) on page 163](#)
- [Viewing Statistics for Specific Device Drivers \(SRC CLI\) on page 164](#)
- [Viewing Statistics for Subscriber and Service Sessions \(SRC CLI\) on page 166](#)
- [Monitoring Statistics for Subscriber and Service Sessions \(SRC CLI\) on page 166](#)

Viewing Statistics About the Directory (SRC CLI)

Purpose View statistics about the directory.

Action user@host> show sae statistics directory

```
SNMP Statistics
Services read      51
Services written   0
Subscriptions read 0
Subscriptions written 0
Users read         0
Users written      0
```

- See Also**
- [Configuring the Directory Location for SAE Data \(C-Web Interface\)](#)
 - [Viewing Statistics for Directory Connections \(SRC CLI\) on page 157](#)
 - [Viewing SNMP Statistics for the Directory \(C-Web Interface\) on page 184](#)
 - [Viewing SNMP Statistics for Directory Connections \(C-Web Interface\) on page 185](#)

Viewing Statistics for Directory Connections (SRC CLI)

Purpose View information for all or specific directory connections.

Action To view statistics for directory connections:

user@host> show sae statistics directory connections

```
DES connection
Connection ID      FEEDBACK_DATA_MANAGER
Number of read     93
Number of write    93
Number of events sent 0
Number of events dropped 0
Average read time  2
Average write time 23
Directory host     127.0.0.1
Directory port     389
Directory type     primary
Primary restore time 83218
Event queue length 0
```

...

```
DES connection
Connection ID      1dapAuth-LdapAuthenticator
Number of read     0
Number of write    0
```

```

Number of events sent      0
Number of events dropped  0
Average read time         0
Average write time        0
Directory host            127.0.0.1
Directory port            389
Directory type            primary
Primary restore time      83200
Event queue length        0

```

To view information about particular directory connections, specify all or part of the connection ID.

```
user@host> show sae statistics directory connections filter filter
```

For example, if you wanted to view the directory connection that contained ldap in its connection ID:

```
user@host> show sae statistics directory connections filter ldap
```

```

DES connection
Connection ID          ldapAuth-LdapAuthenticator
Number of read         0
Number of write        0
Number of events sent  0
Number of events dropped 0
Average read time      0
Average write time     0
Directory host         127.0.0.1
Directory port         389
Directory type         primary
Primary restore time   83608
Event queue length     0

```

To view only the directory connection IDs:

```
user@host> show sae statistics directory connections brief
```

```

Directory Connections
FEEDBACK_DATA_MANAGER
EQUIPMENT_DATA_MANAGER
POM_Engine
LICENSE_MANAGER
SAE_ConfigMgr
adminLdap-LdapAuthenticator
SERVICE_DATA_MANAGER
USER_DATA_MANAGER
SAE_ConfigMgr(dynamicProps)
ldapAuth-LdapAuthenticator

```

- See Also**
- [Configuring the Directory Location for SAE Data \(C-Web Interface\)](#)
 - [Viewing Statistics About the Directory \(SRC CLI\) on page 156](#)
 - [Viewing SNMP Statistics for the Directory \(C-Web Interface\) on page 184](#)
 - [Viewing SNMP Statistics for Directory Connections \(C-Web Interface\) on page 185](#)

Viewing SNMP Information for Client Licenses (SRC CLI)

Purpose View SNMP information about the state of client licenses.

Action user@host> `show sae statistics license client`

- See Also**
- [Configuring SAE Properties for Global Default SNMP Communities for Use with JunosE Routers and Devices Running Junos OS](#)
 - [Viewing SNMP Statistics for Licenses by Device \(C-Web Interface\) on page 186](#)
 - [Viewing SNMP Statistics for Local Licenses \(C-Web Interface\) on page 188](#)
 - [Viewing SNMP Statistics for Client Licenses \(C-Web Interface\) on page 186](#)
 - [Viewing SNMP Information for Local Licenses \(SRC CLI\) on page 159](#)

Viewing SNMP Information for Local Licenses (SRC CLI)

Purpose View SNMP information about the state of local licenses.

Action user@host> `show sae statistics license local`

```
Local License State
Mode                               Client
License server is available       true
Number of licensed service session 300
```

- See Also**
- [Configuring SAE Properties for Global Default SNMP Communities for Use with JunosE Routers and Devices Running Junos OS](#)
 - [Viewing SNMP Statistics for Licenses by Device \(C-Web Interface\) on page 186](#)
 - [Viewing SNMP Statistics for Local Licenses \(C-Web Interface\) on page 188](#)
 - [Viewing SNMP Statistics for Client Licenses \(C-Web Interface\) on page 186](#)

- [Viewing SNMP Information for Licenses on Virtual Routers \(SRC CLI\) on page 160](#)

Viewing SNMP Information for Licenses on Virtual Routers (SRC CLI)

Purpose View SAE license information for the SRC software.

Action To view SNMP information about the state of licenses on specified virtual routers:

```
user@host> show sae statistics license device
```

To view information about the state of licenses for a particular virtual router, specify all or part of the VR name. For device drivers running Junos OS and PCMM drivers, use the format default@routerName.

```
user@host> show sae statistics license device name name
```

To view only the virtual router names:

```
user@host> show sae statistics license device brief
```

- See Also**
- [Configuring SAE Properties for Global Default SNMP Communities for Use with JunosE Routers and Devices Running Junos OS](#)
 - [Viewing SNMP Statistics for Local Licenses \(C-Web Interface\) on page 188](#)
 - [Viewing SNMP Statistics for Client Licenses \(C-Web Interface\) on page 186](#)
 - [Viewing SNMP Information for Local Licenses \(SRC CLI\) on page 159](#)
 - [Viewing SNMP Information for Client Licenses \(SRC CLI\) on page 159](#)

Viewing SNMP Information for Policies (SRC CLI)

Purpose View SNMP information for the policy engine, policy decision point, and the shared object repository where the policy objects are stored:

Action user@host> show sae statistics policy-management

```
SNMP Statistics
Policy Management Type                                Policy Engine Data
Total number of policy group modifications            0
Total number of interface classifier modifications    0
Average time for processing policy group modification 0
Average time for processing interface classifier modification 0
Policy Management Type                                PDP Data
Total number of default policy decisions              45
Total number of service policy decisions              0
Total number of errors                                0
Policy Management Type                                Repository Data
Current total number of policy groups loaded          1
```

- See Also**
- *Configuring SAE Properties for Global Default SNMP Communities for Use with JunosE Routers and Devices Running Junos OS*
 - [Viewing Information About Policies \(C-Web Interface\) on page 172](#)
 - [Viewing SNMP Statistics About Policies \(C-Web Interface\) on page 188](#)

Viewing SNMP Information for the SAE Server Process (SRC CLI)

Purpose View SNMP information for the SAE server process.

Action user@host> show sae statistics process

```
SNMP Statistics
Heap in use 19211 kilo bytes (2%)
Heap limit 910016 kilo bytes
Threads 96
Up time 80877 seconds since Tue Jan 23 19:51:42 EST 2007
```

- See Also**
- *Configuring SAE Properties for Global Default SNMP Communities for Use with JunosE Routers and Devices Running Junos OS*
 - [Viewing SNMP Statistics About Server Processes \(C-Web Interface\) on page 189](#)

Viewing Statistics for RADIUS Clients (SRC CLI)

Purpose View SNMP statistics for RADIUS clients.

Action user@host> **show sae statistics radius**

```
SNMP Statistics
Accounting ACKs from unrecognized IP    0
Authentication ACKs from unrecognized IP 0
Radius client ID                        SAE.buffy
```

- See Also**
- *Configuring the RADIUS Local IP Address and NAS ID (C-Web Interface)*
 - [Viewing SNMP Information for RADIUS Clients \(SRC CLI\) on page 162](#)

Viewing SNMP Information for RADIUS Clients (SRC CLI)

Purpose View SNMP information for RADIUS clients. You can view information for all accounting or authentication clients, or by IP address, UDP port number, or IP address and UDP port.

Action To view SNMP information for RADIUS accounting clients:

```
user@host> show sae statistics radius client accounting
```

To view SNMP information for RADIUS authentication clients:

```
user@host> show sae statistics radius client authentication
```

To view information for a particular RADIUS client by IP address:

```
user@host> show sae statistics radius client ip-address ip-address
user@host> show sae statistics radius client accounting ip-address ip-address
user@host> show sae statistics radius client authentication ip-address ip-address
```

To view information for a particular RADIUS client by UDP port number:

```
user@host> show sae statistics radius client udp-port udp-port
user@host> show sae statistics radius client accounting udp-port udp-port
user@host> show sae statistics radius client authentication udp-port udp-port
```

To view only the RADIUS clients that were accessible by IP address and port number:

```
user@host> show sae statistics radius client brief
user@host> show sae statistics radius client accounting brief
user@host> show sae statistics radius client authentication brief
```


- See Also**
- [Configuring the RADIUS Local IP Address and NAS ID \(C-Web Interface\)](#)
 - [Viewing Statistics for RADIUS Clients \(SRC CLI\) on page 161](#)

Viewing SNMP Information for Routers and Devices (SRC CLI)

Purpose View SNMP information for routers and devices that the SAE manages. You can view information for all routers and devices, or for specific ones.

Action To view SNMP information for routers and devices that the SAE is managing:

```
user@host> show sae statistics device
```

To view information for a particular router, specify all or part of the VR name. For device drivers running Junos OS and PCMM drivers, use the format default@routerName.

```
user@host> show sae statistics device filter filter
```

To view only the RADIUS clients that were accessible by IP address and port number:

```
user@host> show sae statistics device brief
```

- See Also**
- [Configuring SAE Properties for Global Default SNMP Communities for Use with JunosE Routers and Devices Running Junos OS](#)
 - [Viewing Statistics for Device Drivers \(SRC CLI\) on page 163](#)
 - [Viewing SNMP Information for Licenses on Virtual Routers \(SRC CLI\) on page 160](#)
 - [Viewing Statistics for Specific Device Drivers \(SRC CLI\) on page 164](#)

Viewing Statistics for Device Drivers (SRC CLI)

Purpose View SNMP statistics for all device drivers.

Action user@host> show sae statistics device common

```
SNMP Statistics
Driver type          JunosE COPS
Number of close requests 0
Number of connections accepted 0
Number of current connections 0
Number of open requests 0
Server address       0.0.0.0
Server port          3288
Time since last redirect 0
```

```
SNMP Statistics
Driver type          PACKETCABLE COPS
Number of close requests 0
Number of connections accepted 0
Number of current connections 0
Number of open requests 0
Server address       0.0.0.0
Server port          0
Time since last redirect 0
```

```
SNMP Statistics
Driver type          Junos
Number of close requests 0
Number of connections accepted 0
Number of current connections 0
Number of open requests 0
Server address       0.0.0.0
Server port          3333
Time since last redirect 0
```

The value of the server address can be either an IPv4 or IPv6 address, depending on the platform.

- See Also**
- *Shutting Down the Device Drivers (C-Web Interface)*
 - [Viewing Information About SAE Device Drivers \(SRC CLI\) on page 134](#)
 - [Viewing SNMP Information for Routers and Devices \(SRC CLI\) on page 163](#)
 - [Viewing Statistics for Specific Device Drivers \(SRC CLI\) on page 164](#)

Viewing Statistics for Specific Device Drivers (SRC CLI)

Purpose View statistics for specific router drivers or device drivers.

Action To view SNMP statistics for device drivers running Junos OS:

```
user@host> show sae statistics device common junos
```

To view SNMP statistics for JunosE router drivers:

```
user@host> show sae statistics device common junose
```

To view SNMP statistics for PCMM device drivers:

```
user@host> show sae statistics device common packetcable-cops
```

To view SNMP statistics for third-party device drivers:

```
user@host> show sae statistics device common proxy
```

To view SNMP statistics for AAA device drivers:

```
user@host> show sae statistics device common aaa
```

To view SNMP statistics for intelligent service edge device drivers:

```
user@host> show sae statistics device common junos-ise
```

To view SNMP statistics for Device Management Interface (DMI) device drivers:

```
user@host> show sae statistics device common junos-dmi
```

To view SNMP statistics for Gx router drivers:

```
user@host> show sae statistics device common junos-gx
```

For example, to view SNMP statistics for device drivers running Junos OS:

```
user@host> show sae statistics device common junos
```

SNMP Statistics

Driver type	Junos OS
Number of close requests	0
Number of connections accepted	0
Number of current connections	0
Number of open requests	0
Server address	0.0.0.0

Server port	3333
Time since last redirect	0

- See Also**
- [Configuring the Session Store Feature \(SRC CLI\)](#)
 - [Viewing Information About SAE Device Drivers \(SRC CLI\)](#) on page 134
 - [Viewing SNMP Information for Routers and Devices \(SRC CLI\)](#) on page 163
 - [Viewing Statistics for Device Drivers \(SRC CLI\)](#) on page 163

Viewing Statistics for Subscriber and Service Sessions (SRC CLI)

Purpose View SNMP statistics for subscriber and service sessions.

Action user@host> `show sae statistics sessions`

```
SNMP Statistics
Current service sessions           0
Current user sessions              0
Logins (includes sync. and static IP portal logins) 0
Logouts                           0
Service session idle timeouts      0
Service sessions started           0
Service sessions stopped           0
Service session timeouts           0
```

- See Also**
- [Configuring Access to Subscriber Data \(SRC CLI\)](#)
 - [Configuring Access to Service Data \(SRC CLI\)](#)
 - [Viewing Information About Subscriber Sessions by DN \(SRC CLI\)](#) on page 147
 - [Viewing Information About Subscriber Sessions by Service Name \(SRC CLI\)](#) on page 151
 - [Viewing Information About Subscriber Sessions by Session ID \(SRC CLI\)](#) on page 152
 - [Monitoring Statistics for Subscriber and Service Sessions \(SRC CLI\)](#) on page 166

Monitoring Statistics for Subscriber and Service Sessions (SRC CLI)

Purpose Display real-time SNMP statistics for subscriber and service sessions.

Action To display real-time SNMP statistics for subscriber and service sessions:

```
user@host> monitor sae statistics sessions
```

To specify the time interval for refreshing the data:

```
user@host> monitor sae statistics sessions interval interval
```

- See Also**
- [Viewing Statistics for Subscriber and Service Sessions \(SRC CLI\) on page 166](#)
 - *Output Control Keys for monitor Command*

CHAPTER 16

Monitoring SAE Data (C-Web Interface)

- [Viewing SAE Data \(C-Web Interface\) on page 169](#)
- [Viewing Information About Subscriber Sessions \(C-Web Interface\) on page 177](#)
- [Viewing SNMP Information \(C-Web Interface\) on page 184](#)

Viewing SAE Data (C-Web Interface)

You can view data currently stored in the SAE server's memory by:

- [Viewing Information About the Directory Blacklist \(C-Web Interface\) on page 169](#)
- [Viewing Information About Services \(C-Web Interface\) on page 170](#)
- [Viewing Information About Licenses \(C-Web Interface\) on page 171](#)
- [Viewing Information About Policies \(C-Web Interface\) on page 172](#)
- [Viewing Information About Device Drivers \(C-Web Interface\) on page 172](#)
- [Viewing Information About Interfaces \(C-Web Interface\) on page 174](#)
- [Viewing Equipment Registrations \(C-Web Interface\) on page 174](#)
- [Viewing Login Registrations \(C-Web Interface\) on page 176](#)
- [Viewing Information About Threads \(C-Web Interface\) on page 177](#)

Viewing Information About the Directory Blacklist (C-Web Interface)

Purpose View information about the directory blacklist configured on the SAE.

Action 1. Click **Monitor>SAE >Directory Blacklist**.
The Directory Blacklist pane appears.

Figure 12: C-Web Interface for Monitoring SAE Directory Blacklist

2. In the Slot box, enter the number of the slot for which you want to display directory blacklist information.

The Directory Blacklist pane displays the directory blacklist information.

- See Also**
- [Removing the Directory Blacklist \(C-Web Interface\)](#)
 - [Viewing Information About the Directory Blacklist \(SRC CLI\)](#) on page 133

Viewing Information About Services (C-Web Interface)

Purpose View information about the services available on the SAE.

- Action**
1. Click **Monitor>SAE>Services**.
- The Services pane appears.

Figure 13: C-Web Interface for Monitoring SAE Services

2. In the Maximum Results box, enter the maximum number of results that you want to receive.

3. In the Service Name box, enter a full or partial service name for which you want to display information, or leave the box blank to display all services.
4. Select the **Secret** check box to set a flag indicating that secret services are displayed.
5. In the Slot box, enter the number of the slot for which you want to display services information.
6. Select an output style from the Style list.
7. Click **OK**.

The Services pane displays the status of the services running on the SAE.

See Also • [Viewing Information About Services \(SRC CLI\) on page 141](#)

Viewing Information About Licenses (C-Web Interface)

Purpose View information about licenses.

Action 1. Click **Monitor>SAE >Licenses**.

The Licenses pane appears.

Figure 14: C-Web Interface for Monitoring SAE Licenses



2. In the Slot box, enter the number of the slot for which you want to display license information.
3. Click **OK**.

The Licenses pane displays license information.

See Also • [Viewing SNMP Statistics for Licenses by Device \(C-Web Interface\) on page 186](#)
 • [Viewing SNMP Statistics for Local Licenses \(C-Web Interface\) on page 188](#)
 • [Viewing SNMP Statistics for Client Licenses \(C-Web Interface\) on page 186](#)

- Viewing SNMP Information for Local Licenses (SRC CLI) on page 159
- Viewing SNMP Information for Client Licenses (SRC CLI) on page 159

Viewing Information About Policies (C-Web Interface)

Purpose View information about the policies available on the SAE.

Action 1. Click **Monitor>SAE >Policies**.

The Policies pane appears.

Figure 15: C-Web Interface for Monitoring SAE Policies

Field	Description	Value	Legal range	Default
Policy Group	Name of a policy group.	All or part of the policy group name	No value	No value
Maximum Results	Number of results to be displayed.	1..INF	25	25
Slot	Display SAE information for a specified slot.	Currently the chassis has only one slot. The valid value is 0.	0	0
Style	Output style.	Choices: brief; Display only policy group names	detail	detail

- In the Policy Group box, enter a full or partial policy name for which you want to display information, or leave the box blank to display all policies.
- In the Maximum Results box, enter the maximum number of results that you want to receive.
- In the Slot box, enter the number of the slot for which you want to display policy information.
- Select an output style from the Style list.
- Click **OK**.

The Policies pane displays the status of the policies configured on the SAE.

- See Also**
- *Configuring Access to Policy Data (SRC CLI)*
 - Viewing SNMP Information for Policies (SRC CLI) on page 160
 - Viewing SNMP Statistics About Policies (C-Web Interface) on page 188

Viewing Information About Device Drivers (C-Web Interface)

Purpose View information about the device drivers available on the SAE.

Action 1. Click **Monitor>SAE >Drivers**.

The Drivers pane appears.

Figure 16: C-Web Interface for Monitoring SAE Device Drivers

The screenshot shows the Juniper C-Web Interface. The top navigation bar includes 'Monitor', 'Configure', 'Diagnose', and 'Manage'. The 'Monitor' section is expanded, showing 'SAE' and 'Drivers'. The 'Drivers' pane is active, displaying a form with the following fields: 'Device Name' (text input), 'Maximum Results' (text input), 'Slot' (text input with a value of 0), and 'Style' (dropdown menu). Below these fields are 'OK' and 'Reset' buttons. The footer of the interface displays 'Copyright © 2007, Juniper Networks, Inc. All Rights Reserved. Trademark Notice Privacy' and the Juniper logo.

2. In the Device Name box, enter a full or partial device driver name for which you want to display information, or leave the box blank to display all devices.

For JunosE router drivers, use the format:

<virtual router name>@<router name>

For device drivers running Junos OS and PCMM drivers, use the format:

default@<router name>

3. In the Maximum Results box, enter the maximum number of results that you want to receive.

4. In the Slot box, enter the number of the slot for which you want to display device information.

5. Select an output style from the Style list.

6. Click **OK**.

The Drivers pane displays the status of the devices running on the SAE.

See Also • *Connections to Managed Devices*

- [Viewing SNMP Information for Routers and Devices \(SRC CLI\) on page 163](#)
- [Viewing Statistics for Device Drivers \(SRC CLI\) on page 163](#)
- [Viewing Statistics for Specific Device Drivers \(SRC CLI\) on page 164](#)
- [Viewing Information About SAE Device Drivers \(SRC CLI\) on page 134](#)

Viewing Information About Interfaces (C-Web Interface)

Purpose View information about the interfaces available on the router.

Action 1. Click **Monitor>SAE >Interfaces**.

The Interfaces pane appears.

Figure 17: C-Web Interface for Monitoring SAE Interfaces

Field	Description	Value	Default
Interface Name	Name of router interface.	All or part of the interface name	No value
Maximum Results	Number of results to be displayed.	Legal range: 1..INF	25
Slot	Display SAE information for a specified slot.	Currently the chassis has only one slot. The valid value is 0.	0
Style	Output style.	Choices: brief; Display only interface names	Detail
Virtual Router	Name of virtual router.	All or part of the virtual router name	No value

- In the Interface Name box, enter the name of the router interface for which you want to display information, or leave the box blank to display information about all router interfaces.
- In the Maximum Results box, enter the maximum number of results that you want to receive.
- In the Slot box, enter the number of the slot for which you want to display interface information.
- Select an output style from the Style list.
- In the Virtual Router box, enter the name of the virtual router for which you want to display interfaces, or leave the box blank to display information for all virtual routers.
- Click **OK**.

The Interfaces pane displays the interfaces available on the router.

See Also

- [Viewing Information About SAE Interfaces \(SRC CLI\) on page 136](#)
- [External Interfaces on a C Series Controller Overview](#)

Viewing Equipment Registrations (C-Web Interface)

Purpose You can view all equipment registrations, or you can view a specific registration.

Action To view information about equipment registrations.

1. Click **Monitor>SAE >Registered>Equipment**.

The Registered/Equipment pane appears.

Figure 18: C-Web Interface for Monitoring Equipment Registrations

Field	Description	Value	Default
Mac Address	MAC address of equipment registrations.	MAC address in the format xx:xx:xx:xx:xx:xx	No value
Maximum Results	Number of results to be displayed.	Legal range: 1..INF	25
Slot	Display SAE information for a specified slot.	Value: Currently the chassis has only one slot. The valid value is 0.	0
Style	Output style.	Choices: brief: Display only MAC address of registered equipment	Detail

2. In the MAC Address box, enter a MAC address that specifies the equipment registrations that you want to display.

Use the format:

xx:xx:xx:xx:xx:xx

3. In the Maximum Results box, enter the maximum number of results that you want to receive.
4. In the Slot box, enter the number of the slot for which you want to display equipment registration information.
5. Select an output style from the Style list.
6. Click **OK**.

The Registered/Equipment pane displays information about the equipment registrations.

For information about login and equipment registrations, see the *SRC PE Sample Applications Guide*.

- See Also**
- [Removing Login Registrations \(C-Web Interface\)](#)
 - [Removing Equipment Registrations \(C-Web Interface\)](#)
 - [Viewing Login Registrations \(SRC CLI\) on page 140](#)
 - [Viewing Login Registrations \(C-Web Interface\) on page 176](#)

Viewing Login Registrations (C-Web Interface)

Purpose You can view all login registrations, or you can view a specific registration.

Action To view information about login registrations:

1. Click **Monitor>SAE >Registered>Login**.

The Registered/Login pane appears.

Figure 19: C-Web Interface for Monitoring Login Registrations

The screenshot shows the C-Web Interface for Monitoring Login Registrations. The interface has a sidebar on the left with navigation options: ACP, CLI, Component, Date, Disk, Interfaces..., Iptables..., JPS, NIC, NTP, Redirect Server, Route..., SAE, Security, and System. The main content area is titled "Registered / Login" and contains four input fields: "Mac Address", "Maximum Results", "Slot", and "Style". Each field has a description and default value. The "Mac Address" field is highlighted with a tooltip showing the format "xx:xx:xx:xx:xx:xx". Below the fields are "OK" and "Reset" buttons.

2. In the MAC Address box, enter a MAC address that specifies the login registrations that you want to display.

Use the format:

xx:xx:xx:xx:xx:xx

3. In the Maximum Results box, enter the maximum number of results that you want to receive.
4. In the Slot box, enter the number of the slot for which you want to display login registration information.
5. Select an output style from the Style list.
6. Click **OK**.

The Registered/Login pane displays information about the login registrations.

For information about login and equipment registrations, see the *SRC PE Sample Applications Guide*.

- See Also**
- *Removing Login Registrations (C-Web Interface)*
 - *Removing Equipment Registrations (C-Web Interface)*

- [Viewing Login Registrations \(SRC CLI\) on page 140](#)
- [Viewing Equipment Registrations \(C-Web Interface\) on page 174](#)

Viewing Information About Threads (C-Web Interface)

Purpose View information about the threads and their priority on the SAE.

Action 1. Click **Monitor>SAE >Threads**.

The Threads pane appears.

Figure 20: C-Web Interface for Monitoring SAE Threads



2. In the Slot box, enter the number of the slot for which you want to display thread information.
3. Click **OK**.

The Threads pane displays information about threads.

See Also • [Viewing Information About Threads \(SRC CLI\) on page 144](#)

Viewing Information About Subscriber Sessions (C-Web Interface)

- [Information about Subscriber Sessions on page 178](#)
- [Viewing Information About Subscriber Sessions by DN \(C-Web Interface\) on page 178](#)
- [Viewing Information About Subscriber Sessions by IP Address \(C-Web Interface\) on page 179](#)
- [Viewing Information About Subscriber Sessions by Login Name \(C-Web Interface\) on page 180](#)

- [Viewing Information About Subscriber Sessions by Service Name \(C-Web Interface\) on page 181](#)
- [Viewing Information About Subscriber Sessions by Session ID \(C-Web Interface\) on page 182](#)

Information about Subscriber Sessions

You can list subscriber sessions by the distinguished name (DN) of the subscriber entry in the directory, by login name, or by session ID. You can also list subscriber sessions by IP address for Dynamic Host Configuration Protocol (DHCP) subscribers, authenticated Point-to-Point Protocol (PPP) subscribers, and static IP subscribers who are being managed by the SAE.

- See Also**
- [Viewing Information About Subscriber Sessions by DN \(C-Web Interface\) on page 178](#)
 - [Viewing Information About Subscriber Sessions by DN \(SRC CLI\) on page 147](#)
 - [Viewing Information About Subscriber Sessions by IP Address, VPN Identifier, or both \(SRC CLI\) on page 148](#)
 - [Viewing Information About Subscriber Sessions by Login Name \(C-Web Interface\) on page 180](#)
 - [Viewing Information About Subscriber Sessions by Login Name \(SRC CLI\) on page 150](#)
 - [Viewing Information About Subscriber Sessions by Service Name \(C-Web Interface\) on page 181](#)
 - [Viewing Information About Subscriber Sessions by Service Name \(SRC CLI\) on page 151](#)
 - [Viewing Information About Subscriber Sessions by Session ID \(C-Web Interface\) on page 182](#)
 - [Viewing Information About Subscriber Sessions by Session ID \(SRC CLI\) on page 152](#)

Viewing Information About Subscriber Sessions by DN (C-Web Interface)

Purpose View information about subscriber sessions by DN.

Action 1. Click **Monitor>SAE >Subscribers>DN**.

The Subscribers/DN pane appears.

Figure 21: C-Web Interface for Monitoring SAE Subscriber Sessions by DN

Field	Description
Subscriber DN	DN of the subscribers. Value: All or part of the subscriber DN Default: No value
Maximum Results	Number of results to be displayed. Legal range: 1..INF Default: 25
Secret	Display subscriber sessions and service sessions for hidden services. Default: Disabled
Slot	Display SAE information for a specified slot. Value: Currently the chassis has only one slot. The valid value is 0. Default: 0
Style	Output style Choices: brief: Display only subscriber sessions terse: Display subscriber session ID, login name, and IP address Default: Detail

- In the Subscriber DN box, enter a full or partial subscriber DN for which you want to display information, or leave the box blank to display all subscriber sessions.
- In the Maximum Results box, enter the maximum number of results that you want to receive.
- Select the **Secret** check box to set a flag indicating that subscriptions and service sessions from hidden services are displayed.
- In the Slot box, enter the number of the slot for which you want to display subscriber session information.
- Select an output style from the Style list.
- Click **OK**.

The Subscribers/DN pane displays information about subscriber sessions.

- See Also**
- [Configuring Access to Subscriber Data \(SRC CLI\)](#)
 - [Viewing Information About Subscriber Sessions by IP Address \(C-Web Interface\) on page 179](#)
 - [Viewing Information About Subscriber Sessions by Login Name \(C-Web Interface\) on page 180](#)
 - [Viewing Information About Subscriber Sessions by Service Name \(C-Web Interface\) on page 181](#)
 - [Viewing Information About Subscriber Sessions by Session ID \(C-Web Interface\) on page 182](#)

Viewing Information About Subscriber Sessions by IP Address (C-Web Interface)

Purpose View information about subscriber sessions by IP address.

Action 1. Click **Monitor>SAE >Subscribers>IP**.

The Subscribers/IP pane appears.

Figure 22: C-Web Interface for Monitoring SAE Subscriber Sessions by IP Address

Field	Description	Default
IP Address	IP address of subscriber sessions. Value: All or part of the subscriber IP address	No value
Maximum Results	Number of results to be displayed. Legal range: 1..INF	25
Secret	Display subscriber sessions and service sessions for hidden services.	Disabled
Slot	Display SAE information for a specified slot. Value: Currently the chassis has only one slot. The valid value is 0.	0
Style	Output style Choices: brief: Display only subscriber sessions terse: Display subscriber session ID, login name, and IP address	Detail

- In the IP Address box, enter a full or partial IP address for which you want to display information, or leave the box blank to display all subscriber sessions.
- In the Maximum Results box, enter the maximum number of results that you want to receive.
- Select the **Secret** check box to set a flag indicating that subscriptions and service sessions from hidden services are displayed.
- In the Slot box, enter the number of the slot for which you want to display subscriber session information.
- Select an output style from the Style list.
- Click **OK**.

The Subscribers/IP pane displays information about subscriber sessions.

- See Also**
- [Configuring Access to Subscriber Data \(SRC CLI\)](#)
 - [Viewing Information About Subscriber Sessions by DN \(C-Web Interface\) on page 178](#)
 - [Viewing Information About Subscriber Sessions by Login Name \(C-Web Interface\) on page 180](#)
 - [Viewing Information About Subscriber Sessions by Service Name \(C-Web Interface\) on page 181](#)
 - [Viewing Information About Subscriber Sessions by Session ID \(C-Web Interface\) on page 182](#)

Viewing Information About Subscriber Sessions by Login Name (C-Web Interface)

Purpose View information about subscriber sessions by login name.

Action 1. Click **Monitor>SAE >Subscribers>Login Name**.

The Subscribers/Login Name pane appears.

Figure 23: C-Web Interface for Monitoring SAE Subscriber Sessions by Login Name

Field	Description	Default
Login Name	Login name of subscriber sessions. Value: All or part of the subscriber login name	No value
Maximum Results	Number of results to be displayed. Legal range: 1..INF	25
Secret	Display subscriber sessions and service sessions for hidden services.	Disabled
Slot	Display SAE information for a specified slot. Value: Currently the chassis has only one slot. The valid value is 0.	0
Style	Output style Choices: brief: Display only subscriber sessions terse: Display subscriber session ID, login name, and IP address	Detail

- In the Login Name box, enter a full or partial login name for which you want to display information, or leave the box blank to display all subscriber sessions.
- In the Maximum Results box, enter the maximum number of results that you want to receive.
- Select the **Secret** check box to set a flag indicating that subscriptions and service sessions from hidden services are displayed.
- In the Slot box, enter the number of the slot for which you want to display subscriber session information.
- Select an output style from the Style list.
- Click **OK**.

The Subscribers/Login Name pane displays information about subscriber sessions.

- See Also**
- *Configuring Access to Subscriber Data (SRC CLI)*
 - [Viewing Information About Subscriber Sessions by DN \(C-Web Interface\) on page 178](#)
 - [Viewing Information About Subscriber Sessions by IP Address \(C-Web Interface\) on page 179](#)
 - [Viewing Information About Subscriber Sessions by Service Name \(C-Web Interface\) on page 181](#)
 - [Viewing Information About Subscriber Sessions by Session ID \(C-Web Interface\) on page 182](#)

Viewing Information About Subscriber Sessions by Service Name (C-Web Interface)

Purpose View information about subscriber sessions by service name.

Action 1. Click **Monitor>SAE >Subscribers>Service Name**.

The Subscribers/Service Name pane appears.

Figure 24: C-Web Interface for Monitoring SAE Subscriber Sessions by Service Name

Field	Description	Default
Service Name	Service name of subscriber sessions. Value: All or part of the service name	No value
Maximum Results	Number of results to be displayed. Legal range: 1..INF	25
Secret	Display subscriber sessions and service sessions for hidden services.	Disabled
Slot	Display SAE information for a specified slot. Value: Currently the chassis has only one slot. The valid value is 0.	0
Style	Output style Choices: brief: Display only subscriber sessions terse: Display subscriber session ID, login name, and IP address	Detail

- In the Service Name box, enter a full or partial service name for which you want to display information, or leave the box blank to display all subscriber sessions.
- In the Maximum Results box, enter the maximum number of results that you want to receive.
- Select the **Secret** check box to set a flag indicating that subscriptions and service sessions from hidden services are displayed.
- In the Slot box, enter the number of the slot for which you want to display subscriber session information.
- Select an output style from the Style list.
- Click **OK**.

The Subscribers/Service Name pane displays information about subscriber sessions.

- See Also**
- [Configuring Access to Subscriber Data \(SRC CLI\)](#)
 - [Viewing Information About Subscriber Sessions by DN \(C-Web Interface\) on page 178](#)
 - [Viewing Information About Subscriber Sessions by IP Address \(C-Web Interface\) on page 179](#)
 - [Viewing Information About Subscriber Sessions by Login Name \(C-Web Interface\) on page 180](#)
 - [Viewing Information About Subscriber Sessions by Session ID \(C-Web Interface\) on page 182](#)

Viewing Information About Subscriber Sessions by Session ID (C-Web Interface)

Purpose View information about subscriber sessions by session ID.

Action 1. Click **Monitor>SAE >Subscribers>Session ID**.

The Subscribers/Session ID pane appears.

Figure 25: C-Web Interface for Monitoring SAE Subscriber Sessions by Session ID

Field	Description	Value	Default
Session ID	ID of subscriber sessions.	All or part of the subscriber session ID	No value
Maximum Results	Number of results to be displayed.	Legal range: 1..INF	25
Secret	Display subscriber sessions and service sessions for hidden services.	Disabled	Disabled
Slot	Display SAE information for a specified slot.	Currently the chassis has only one slot. The valid value is 0.	0
Style	Output style	Choices: brief: Display only subscriber sessions; terse: Display subscriber session ID, login name, and IP address	Detail

- In the Session ID box, enter a full or partial session ID name for which you want to display information, or leave the box blank to display all subscriber sessions.
- In the Maximum Results box, enter the maximum number of results that you want to receive.
- Select the **Secret** check box to set a flag indicating that subscriptions and service sessions from hidden services are displayed.
- In the Slot box, enter the number of the slot for which you want to display subscriber session information.
- Select an output style from the Style list.
- Click **OK**.

The Subscribers/Session ID pane displays information about subscriber sessions.

- See Also**
- [Configuring Access to Subscriber Data \(SRC CLI\)](#)
 - [Viewing Information About Subscriber Sessions by DN \(C-Web Interface\) on page 178](#)
 - [Viewing Information About Subscriber Sessions by IP Address \(C-Web Interface\) on page 179](#)
 - [Viewing Information About Subscriber Sessions by Login Name \(C-Web Interface\) on page 180](#)
 - [Viewing Information About Subscriber Sessions by Service Name \(C-Web Interface\) on page 181](#)

Viewing SNMP Information (C-Web Interface)

You can use the C-Web interface to view SNMP statistics for the SAE configuration by:

- Viewing SNMP Statistics for the Directory (C-Web Interface) on page 184
- Viewing SNMP Statistics for Directory Connections (C-Web Interface) on page 185
- Viewing SNMP Statistics for Client Licenses (C-Web Interface) on page 186
- Viewing SNMP Statistics for Licenses by Device (C-Web Interface) on page 186
- Viewing SNMP Statistics for Local Licenses (C-Web Interface) on page 188
- Viewing SNMP Statistics About Policies (C-Web Interface) on page 188
- Viewing SNMP Statistics About Server Processes (C-Web Interface) on page 189
- Viewing SNMP Statistics About RADIUS (C-Web Interface) on page 190
- Viewing SNMP Statistics About RADIUS Clients (C-Web Interface) on page 191
- Viewing SNMP Statistics for Devices (C-Web Interface) on page 192
- Viewing SNMP Statistics for Specific Devices (C-Web Interface) on page 193
- Viewing SNMP Statistics for Subscriber Sessions and Service Sessions (C-Web Interface) on page 194

Viewing SNMP Statistics for the Directory (C-Web Interface)

Purpose View SNMP statistics for the directory.

Action 1. Click **Monitor>SAE >Statistics>Directory**.

The Statistics/Directory pane appears.

Figure 26: C-Web Interface for Monitoring SNMP Statistics of the Directory



2. In the Slot box, enter the number of the slot for which you want to display SNMP statistics for the directory.

3. Click **OK**.

The Statistics/Directory pane displays statistics for the directory.

- See Also**
- *Configuring SAE Properties for Global Default SNMP Communities for Use with JunosE Routers and Devices Running Junos OS*
 - [Viewing Statistics for Directory Connections \(SRC CLI\) on page 157](#)
 - [Viewing Statistics About the Directory \(SRC CLI\) on page 156](#)
 - [Viewing SNMP Statistics for Directory Connections \(C-Web Interface\) on page 185](#)

Viewing SNMP Statistics for Directory Connections (C-Web Interface)

Purpose View SNMP statistics for directory connections.

- Action** 1. Click **Monitor>SAE >Statistics>Directory>Connections**.

The Statistics/Directory/Connections pane appears.

Figure 27: C-Web Interface for Monitoring SNMP Statistics of Directory Connections

The screenshot shows the Juniper C-Web Interface. The top navigation bar includes 'Monitor', 'Configure', 'Diagnose', and 'Manage'. The 'Monitor' tab is selected, and the left sidebar shows a tree structure with 'SAE' expanded. The main content area is titled 'Statistics / Directory / Connections'. It contains three input fields: 'Connection ID', 'Slot', and 'Style'. Each field has a tooltip explaining its purpose and default value. At the bottom of the form are 'OK' and 'Reset' buttons. The footer of the interface shows the copyright notice for Juniper Networks, Inc. 2007.

- In the Connection ID box, enter a full or partial connection ID for which you want to display information, or leave the box blank to display all SNMP statistics for all directory connections.
- In the Slot box, enter the number of the slot for which you want to display SNMP statistics for directory connections.
- Select an output style from the Style list.
- Click **OK**.

The Statistics/Connections pane displays statistics for directory connections.

- See Also**
- *Configuring SAE Properties for Global Default SNMP Communities for Use with JunosE Routers and Devices Running Junos OS*
 - [Viewing Statistics for Directory Connections \(SRC CLI\) on page 157](#)
 - [Viewing Statistics About the Directory \(SRC CLI\) on page 156](#)
 - [Viewing SNMP Statistics for the Directory \(C-Web Interface\) on page 184](#)

Viewing SNMP Statistics for Client Licenses (C-Web Interface)

Purpose View SNMP statistics for client licenses.

Action 1. Click **Monitor>SAE >Statistics>License>Client**.

The Statistics/License/Client pane appears.

Figure 28: C-Web Interface for Monitoring SNMP Statistics of Client Licenses



2. In the Slot box, enter the number of the slot for which you want to display SNMP statistics for client licenses.

3. Click **OK**.

The Statistics/License/Client pane displays statistics for client licenses.

- See Also**
- [Viewing SNMP Statistics for Licenses by Device \(C-Web Interface\) on page 186](#)
 - [Viewing SNMP Statistics for Local Licenses \(C-Web Interface\) on page 188](#)
 - [Viewing SNMP Information for Local Licenses \(SRC CLI\) on page 159](#)
 - [Viewing SNMP Information for Client Licenses \(SRC CLI\) on page 159](#)
 - [Viewing SNMP Information for Licenses on Virtual Routers \(SRC CLI\) on page 160](#)

Viewing SNMP Statistics for Licenses by Device (C-Web Interface)

Purpose View SNMP statistics for licenses by device.

Action 1. Click **Monitor>SAE >Statistics>License>Device**.

The Statistics/License/Device pane appears.

Figure 29: C-Web Interface for Monitoring SNMP Statistics of Virtual Router Licenses

2. In the Device Name box, enter a full or partial device name for which you want to display information, or leave the box blank to display SNMP statistics for all devices.

For JunosE router drivers, use the format:

<virtual router name>@<router name>

For device drivers running Junos OS and PCMM drivers, use the format:

default@<router name>

3. In the Slot box, enter the number of the slot for which you want to display SNMP statistics for device licenses.

4. Select an output style from the Style list.

5. Click **OK**.

The Statistics/License/Device pane displays statistics for virtual router licenses.

- See Also**
- *Connections to Managed Devices*
 - [Viewing SNMP Information for Local Licenses \(SRC CLI\) on page 159](#)
 - [Viewing SNMP Information for Client Licenses \(SRC CLI\) on page 159](#)
 - [Viewing SNMP Information for Licenses on Virtual Routers \(SRC CLI\) on page 160](#)
 - [Viewing SNMP Statistics for Client Licenses \(C-Web Interface\) on page 186](#)
 - [Viewing SNMP Statistics for Local Licenses \(C-Web Interface\) on page 188](#)

Viewing SNMP Statistics for Local Licenses (C-Web Interface)

Purpose View SNMP statistics for local licenses.

Action 1. Click **Monitor>SAE >Statistics>License>Local**.

The Statistics/License/Local pane appears.

Figure 30: C-Web Interface for Monitoring SNMP Statistics of Local Licenses



2. In the Slot box, enter the number of the slot for which you want to display SNMP statistics for local licenses.

3. Click **OK**.

The Statistics/License/Local pane displays statistics for local licenses.

See Also • *Configuring SAE Properties for Global Default SNMP Communities for Use with JunosE Routers and Devices Running Junos OS*

- [Viewing SNMP Information for Local Licenses \(SRC CLI\) on page 159](#)
- [Viewing SNMP Information for Client Licenses \(SRC CLI\) on page 159](#)
- [Viewing SNMP Information for Licenses on Virtual Routers \(SRC CLI\) on page 160](#)
- [Viewing SNMP Statistics for Client Licenses \(C-Web Interface\) on page 186](#)
- [Viewing SNMP Statistics for Licenses by Device \(C-Web Interface\) on page 186](#)

Viewing SNMP Statistics About Policies (C-Web Interface)

Purpose View SNMP statistics about policies.

Action Click **Monitor>SAE >Statistics>Policy Management**.

The Statistics/Policy Management pane appears.

Figure 31: C-Web Interface for Monitoring SNMP Statistics of Policies



1. In the Slot box, enter the number of the slot for which you want to display SNMP statistics for policies.
2. Click **OK**.

The Statistics/Policy Management pane displays statistics for policies.

- See Also**
- *Configuring SAE Properties for Global Default SNMP Communities for Use with JunosE Routers and Devices Running Junos OS*
 - [Viewing Information About Policies \(C-Web Interface\) on page 172](#)
 - [Viewing SNMP Information for Policies \(SRC CLI\) on page 160](#)

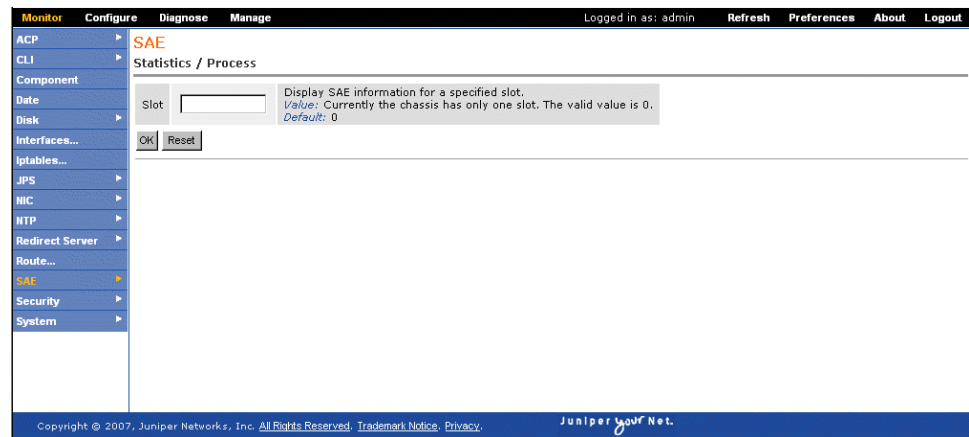
Viewing SNMP Statistics About Server Processes (C-Web Interface)

Purpose View SNMP statistics about server processes.

- Action**
1. Click **Monitor>SAE >Statistics>Process**.

The Statistics/Process pane appears.

Figure 32: C-Web Interface for Monitoring SNMP Statistics of Server Processes



2. In the Slot box, enter the number of the slot for which you want to display SNMP statistics for server processes.
3. Click **OK**.

The Statistics/Process pane displays statistics for server processes.

- See Also**
- *Configuring SAE Properties for Global Default SNMP Communities for Use with JunosE Routers and Devices Running Junos OS*
 - [Viewing SNMP Information for the SAE Server Process \(SRC CLI\) on page 161](#)

Viewing SNMP Statistics About RADIUS (C-Web Interface)

Purpose View SNMP statistics about RADIUS.

- Action** 1. Click **Monitor>SAE >Statistics>RADIUS**.

The Statistics/RADIUS pane appears.

Figure 33: C-Web Interface for Monitoring SNMP Statistics of RADIUS Server



2. In the Slot box, enter the number of the slot for which you want to display SNMP statistics for RADIUS.
3. Click **OK**.

The Statistics/RADIUS pane displays statistics for RADIUS.

- See Also**
- *Configuring SAE Properties for Global Default SNMP Communities for Use with JunosE Routers and Devices Running Junos OS*
 - [Viewing SNMP Statistics About RADIUS Clients \(C-Web Interface\)](#) on page 191

Viewing SNMP Statistics About RADIUS Clients (C-Web Interface)

Purpose View SNMP statistics about RADIUS clients.

- Action** 1. Click **Monitor>SAE >Statistics>RADIUS>Client**.

The Statistics/RADIUS/Client pane appears.

Figure 34: C-Web Interface for Monitoring SNMP Statistics of RADIUS Clients

The screenshot shows the Juniper C-Web Interface. The top navigation bar includes 'Monitor', 'Configure', 'Diagnose', and 'Manage'. The user is logged in as 'admin'. The left sidebar lists various system components. The main pane is titled 'Statistics / RADIUS / Client' and contains the following fields:

- Client Type:** A dropdown menu currently set to 'authentication'. Description: 'Display SNMP information for either RADIUS accounting clients or RADIUS authentication clients. Choices: accounting: Display RADIUS accounting client information; authentication: Display RADIUS authentication client information. Default: No value'.
- Ip Address:** A text input field. Description: 'IP address or addresses of RADIUS clients. Value: All or part of the client IP address. Default: No value'.
- Slot:** A text input field. Description: 'Display SAE information for a specified slot. Value: Currently the chassis has only one slot. The valid value is 0. Default: 0'.
- Style:** A dropdown menu currently set to 'brief'. Description: 'Output style. Choices: brief: Display only clients accessible by IP address/port number; Detail. Default: Detail'.
- Udp Port:** A text input field. Description: 'Port number for RADIUS clients. Value: All or part of the client port number. Default: No value'.

At the bottom of the form, there is a note '*Mandatory' and two buttons: 'OK' and 'Reset'.

2. Select a client type from the Client Type list:
 - accounting—Displays RADIUS accounting information
 - authentication—Displays RADIUS client authentication information
3. In the IP Address box, enter the client IP address to display SNMP information for a specific RADIUS client, or leave the box blank to display SNMP information for all RADIUS clients.
4. In the Slot box, enter the number of the slot for which you want to display SNMP statistics for RADIUS clients.
5. Select an output style from the Style list.

6. In the UDP Port box, enter a port number to display SNMP information for a specific RADIUS client, or leave the box blank to display SNMP information for all RADIUS clients.
7. Click **OK**.

The Statistics/RADIUS/Client pane displays statistics for RADIUS clients.

- See Also**
- *Configuring SAE Properties for Global Default SNMP Communities for Use with JunosE Routers and Devices Running Junos OS*
 - [Viewing SNMP Statistics About RADIUS \(C-Web Interface\) on page 190](#)

Viewing SNMP Statistics for Devices (C-Web Interface)

Purpose View SNMP statistics about devices.

- Action** 1. Click **Monitor>SAE >Statistics>Device**.

The Statistics/Device pane appears.

Figure 35: C-Web Interface for Monitoring SNMP Statistics of Device Drivers

The screenshot displays the Juniper C-Web Interface for Monitoring SNMP Statistics of Device Drivers. The interface is divided into a sidebar and a main content area. The sidebar contains navigation options: Monitor, Configure, Diagnose, and Manage. The main content area is titled "Statistics / Device" and contains three input fields: "Device Name", "Slot", and "Style". The "Device Name" field has a text input box. The "Slot" field has a numeric input box. The "Style" field has a dropdown menu. Below these fields are "OK" and "Reset" buttons. The footer of the interface shows the Juniper logo and copyright information: "Copyright © 2007, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy.".

2. In the Device Name box, enter a full or partial device name for which you want to display information, or leave the box blank to display all devices.
3. In the Slot box, enter the number of the slot for which you want to display SNMP statistics for devices.
4. Select an output style from the Style list.
5. Click **OK**.

The Statistics/Device pane displays statistics for all devices.

- See Also**
- *Configuring SAE Properties for Global Default SNMP Communities for Use with JunosE Routers and Devices Running Junos OS*

- [Viewing SNMP Statistics for Specific Devices \(C-Web Interface\)](#) on page 193
- [Viewing SNMP Statistics for Subscriber Sessions and Service Sessions \(C-Web Interface\)](#) on page 194

Viewing SNMP Statistics for Specific Devices (C-Web Interface)

Purpose View SNMP statistics about specific devices.

Action 1. Click **Monitor>SAE >Statistics>Device>Common**.

The Statistics/Device/Common pane appears.

Figure 36: C-Web Interface for Monitoring SNMP Statistics of a Specific Device Driver Type

- In the Device Name box, enter a full or partial device name for which you want to display information, or leave the box blank to display all devices.
- In the Slot box, enter the number of the slot for which you want to display SNMP statistics for specific devices.
- Select a device type from the Type list:
 - junos—Displays SNMP statistics for device drivers running Junos OS
 - junose-cops—Displays SNMP statistics for JunosE router drivers
 - packetable-COPS—Displays SNMP statistics for PCMM device drivers
 - proxy—Displays SNMP statistics for third-party drivers
- Click **OK**.

The Statistics/Device/Common pane displays statistics for the specified device.

- See Also**
- [Configuring SAE Properties for Global Default SNMP Communities for Use with JunosE Routers and Devices Running Junos OS](#)
 - [Viewing SNMP Statistics for Devices \(C-Web Interface\)](#) on page 192

- [Viewing SNMP Statistics for Subscriber Sessions and Service Sessions \(C-Web Interface\) on page 194](#)

Viewing SNMP Statistics for Subscriber Sessions and Service Sessions (C-Web Interface)

Purpose View SNMP statistics about subscriber sessions and service sessions.

Action 1. Click **Monitor>SAE >Statistics>Sessions**.

The Statistics/Sessions pane displays statistics for subscriber sessions and service sessions.

Figure 37: C-Web Interface for Monitoring SNMP Statistics of Subscriber Sessions and Service Sessions



2. In the Slot box, enter the number of the slot for which you want to display SNMP statistics for specific devices.

3. Click **OK**.

The Statistics/Sessions pane displays statistics for subscriber sessions and service sessions.

- See Also**
- [Configuring SAE Properties for Global Default SNMP Communities for Use with JunosE Routers and Devices Running Junos OS](#)
 - [Viewing SNMP Statistics for Devices \(C-Web Interface\) on page 192](#)
 - [Viewing SNMP Statistics for Specific Devices \(C-Web Interface\) on page 193](#)

Monitoring and Troubleshooting the NIC (SRC CLI)

- [SRC CLI Commands to View Statistics About NIC Operations on page 195](#)
- [Viewing Statistics for the NIC Process \(SRC CLI\) on page 196](#)
- [Viewing Statistics for a NIC Host \(SRC CLI\) on page 197](#)
- [Viewing Statistics for NIC Resolvers \(SRC CLI\) on page 198](#)
- [Viewing Statistics for NIC Agents \(SRC CLI\) on page 199](#)
- [SRC CLI Commands to View NIC Resolution Data on page 201](#)
- [Viewing Data for NIC Resolvers \(SRC CLI\) on page 201](#)
- [Viewing Data for NIC Agents \(SRC CLI\) on page 203](#)
- [Troubleshooting NIC Data Resolution \(SRC CLI\) on page 205](#)

SRC CLI Commands to View Statistics About NIC Operations

You can view statistics for the NIC process and for various NIC components. [Table 27 on page 195](#) lists the commands you use to view NIC statistics.

Table 27: Commands to Display NIC Statistics

Command	Output Displayed
show nic statistics	All NIC statistics. The output for this command includes the output for the other show nic statistics commands.
show nic statistics agent	NIC statistics for agents.
show nic statistics host	NIC statistics for a NIC host.
show nic statistics process	NIC statistics for the NIC process.
show nic statistics resolver	NIC statistics for resolvers.
show nic statistics slot	All NIC statistics for a specified slot. The output for this command includes the output for the show nic statistics agent , show nic statistics host , show nic statistics process , and show nic statistics resolver commands.

- Related Documentation**
- [Configuring the NIC \(SRC CLI\)](#)
 - [Locating Subscriber Management Information](#)
 - [Viewing Statistics for the NIC Process \(SRC CLI\) on page 196](#)
 - [Viewing Statistics for a NIC Host \(SRC CLI\) on page 197](#)
 - [SRC CLI Commands to View NIC Resolution Data on page 201](#)

Viewing Statistics for the NIC Process (SRC CLI)

Purpose View statistics for the NIC process.

Action user@host> **show nic statistics process**

Component Statistics

```
Component Name process
Heap in use      21545 KB (16%)
Heap limit      131072 KB
Threads         38
Up time         313152 seconds since Mon Jan 06 15:20:15 UTC 2014
```

Meaning [Table 28 on page 196](#) describes the output fields for the **show nic statistics process** command. Output fields are listed in the order in which they appear.

Table 28: Output Fields for show nic statistics process

Field Name	Field Description
Component name	Name of component—process indicates the NIC process.
Heap in use	Heap size allocated by the Java Virtual Machine. The percentage indicates the percentage of the heap in use. We recommend that if the percent in use is more than 90% additional heap be allocated for the NIC.
Heap limit	Size of Java heap configured for the NIC.
Threads	Number of threads in use.
Up time	Length of time NIC has been running on the system. Includes the date and time at which NIC was last started.

- Related Documentation**
- [Configuring the NIC \(SRC CLI\)](#)
 - [Viewing Host Process Statistics \(C-Web Interface\) on page 208](#)
 - [Viewing Statistics for a NIC Host \(SRC CLI\) on page 197](#)

- [Viewing Statistics for NIC Resolvers \(SRC CLI\) on page 198](#)
- [Viewing Statistics for NIC Agents \(SRC CLI\) on page 199](#)

Viewing Statistics for a NIC Host (SRC CLI)

Purpose View statistics for a NIC host.

Action `user@host> show nic statistics host`

Component Statistics

```
Component Name           /hosts
Number of Components Restart  0
Number of No Match Resolutions 0
Number of Resolution Errors   0
Number of Resolutions        0
```

Meaning [Table 29 on page 197](#) describes the output fields for the `show nic statistics host` command. Output fields are listed in the order in which they appear.

Table 29: Output Fields for show nic statistics test

Field Name	Field Description
Component name	Name of component—/hosts indicates NIC host. A specific host has the format <code>/hosts/ hostname</code> .
Number of Components Restart	Number of NIC resolvers and agents that have restarted in the host.
Number of No Match Resolutions	Number of resolution requests that did not return data.
Number of Resolution Errors	Number of errors encountered when processing resolutions requests.
Number of Resolutions	Number of successful data resolutions; for example, the SAE reference for a specified IP address, the login name for a specified IP address, or the SAE reference for a specified login name.

- Related Documentation**
- [Configuring the NIC \(SRC CLI\)](#)
 - [Viewing Host Statistics \(C-Web Interface\) on page 207](#)
 - [Viewing Statistics for the NIC Process \(SRC CLI\) on page 196](#)
 - [Viewing Statistics for NIC Resolvers \(SRC CLI\) on page 198](#)

- [Viewing Statistics for NIC Agents \(SRC CLI\) on page 199](#)

Viewing Statistics for NIC Resolvers (SRC CLI)

Purpose View statistics for NIC resolvers.

To interpret the statistics for NIC resolvers, make sure that you have a good understanding of the NIC resolutions process.

See *NIC Resolution Process Overview*.

Action `user@host> show nic statistics resolver`

Component Statistics

Component Name	/realms/login/A1
Number of Data Sources	0
Resolver Size	0

Component Statistics

Component Name	/realms/login/B1
Number of Data Sources	1
Resolver Size	0

Component Statistics

Component Name	/realms/login/C1
Number of Data Sources	1
Resolver Size	2140

Component Statistics

Component Name	/realms/login/D1
Number of Data Sources	2
Resolver Size	0

Meaning [Table 30 on page 199](#) describes the output fields for the `show nic statistics resolver` command. Output fields are listed in the order in which they appear.

Table 30: Output Fields for show nic statistics resolver

Field Name	Field Description
Component name	Name of a resolver. Resolver names have the format <i>/realms/ realm-name/resolver name</i> .
Number of Data Sources	The number of sources from which the resolver obtains data. A data source can be an agent or another resolver.
Resolver Size	The number of keys (or number of mappings) required to perform this resolution.

Related Documentation

- [Configuring the NIC \(SRC CLI\)](#)
- [Viewing Resolver Statistics \(C-Web Interface\) on page 210](#)
- [Viewing Resolvers \(C-Web Interface\) on page 209](#)
- [Viewing Statistics for the NIC Process \(SRC CLI\) on page 196](#)
- [Viewing Statistics for NIC Agents \(SRC CLI\) on page 199](#)

Viewing Statistics for NIC Agents (SRC CLI)

Purpose To interpret the statistics for NIC agents, make sure that you have a good understanding of the NIC agents.

See *Mapping Subscribers to a Managing SAE*.

View statistics for NIC agents.

Action user@host> show nic statistics agent

Component Statistics

Component Name /agents/LoginNameVr
Agent Type Passive
Connection to Data Source Up
Data Size 262141

Component Statistics

Component Name /agents/VrSaeId
Agent Type Active
Connection to Data Source Up
Data Size 2212

Component Statistics

Component Name /agents/IpLoginName
Agent Type Passive
Connection to Data Source Up
Data Size 262141

Component Statistics

Component Name /agents/Pool
Agent Type Active
Connection to Data Source Up
Data Size 3

Meaning [Table 31 on page 200](#) describes the output fields for the **show nic statistics agent** command. Output fields are listed in the order in which they appear.

Table 31: Output Fields for show nic statistics agent

Field Name	Field Description
Component name	Name of an agent. Agent names have the format <code>/agents/ agent-name</code> .
Agent Type	Type of agent—active or passive. Active agents publish data whether or not a resolver requests the data. Passive agents provide information only when a resolver requests it.
Connection to Data Source	Whether or not the agent has a connection to its data source; for example, a directory agent to the directory, or an SAE plug-in agent to the CORBA naming server.
Data Size	Number of key to value mappings for the agent.

- Related Documentation**
- [Configuring a NIC Scenario \(SRC CLI\)](#)
 - [Viewing Agents \(C-Web Interface\) on page 210](#)
 - [Viewing Agent Statistics \(C-Web Interface\) on page 211](#)
 - [Viewing Statistics for the NIC Process \(SRC CLI\) on page 196](#)
 - [Viewing Statistics for NIC Resolvers \(SRC CLI\) on page 198](#)

SRC CLI Commands to View NIC Resolution Data

You can view the data that NIC uses during a resolution. You can view all resolution data, or data for a specified NIC component. [Table 32 on page 201](#) lists the commands you use to view NIC resolution information.

Table 32: Commands to Display NIC Data

Command	Output Displayed
<code>show nic data</code>	All NIC data. The output for this command includes the output for the other <code>show nic data</code> commands.
<code>show nic data maximum-results</code>	All or a specified quantity of NIC resolution data.
<code>show nic data agent</code>	NIC resolution data for a specified agent.
<code>show nic data resolver</code>	NIC resolution data for a specified resolver.
<code>show nic data slot</code>	All NIC data for a specified slot. The output for this command includes the output for the <code>show nic data agent</code> and <code>show nic data resolver</code> commands.

- Related Documentation**
- [Testing a NIC Resolution \(SRC CLI\)](#)
 - [SRC CLI Commands to View Statistics About NIC Operations on page 195](#)
 - [Viewing Data for NIC Resolvers \(SRC CLI\) on page 201](#)
 - [Viewing Data for NIC Agents \(SRC CLI\) on page 203](#)

Viewing Data for NIC Resolvers (SRC CLI)

Purpose View all NIC resolver data.

To interpret the data for resolvers, make sure that you have a good understanding of the NIC resolution process.

See *NIC Resolution Process Overview*.

Action user@host> show nic data resolver

```

Component name
/realms/login/C1
Key
  Type
Vr
  String
default@dw2
Value
  Type
SaeId
  String
IOR:
0000000000000003549444C3A736D67742E6A756E697065722E6E65742F7361652F5365727...
41637469766174696F6E456E67696E653A312E30000000000000020000000000000780...
0000000C31302E3232372E362E343300226100000000000226761726B6269742E6B616E6C6...
6E70722E6E65742F736165504F412F53414500000000000200000000000008000000004...
000000010000001C000000000001000100000001050100010001010900000001050100010...
0000002C0000000000000001000000010000001C000000000001000100000001050100010...
0000000105010001...
Key
  Type
Vr
  String
vr1495@marvin
Value
  Type
SaeId
  String
...

```

Meaning [Table 33 on page 202](#) describes the output fields for the **show nic data resolver** command. Output fields are listed in the order in which they appear.

Table 33: Output Fields for show nic data resolver

Field Name	Field Description
Component name	Name of a resolver. Resolver names have the format <code>/realms/ realm-name/resolver name</code> .
Key	Data type and value of a NIC key. The value is the actual value of the NIC key, not the NIC value to which the key maps.
Value	Data type and value of the NIC value that maps to the associated NIC key.

Related Documentation

- [Viewing Statistics for NIC Resolvers \(SRC CLI\) on page 198](#)
- [Viewing Resolvers \(C-Web Interface\) on page 209](#)
- [Viewing Resolver Statistics \(C-Web Interface\) on page 210](#)

- [Viewing Data for NIC Agents \(SRC CLI\) on page 203](#)

[Viewing Data for NIC Agents \(SRC CLI\)](#)

Purpose To interpret the data for agents, make sure that you have a good understanding of the NIC resolution process.

See *NIC Resolution Process Overview*.

View all NIC resolver data.

Action user@host> show nic data agent

```

Component name
/agents/LoginNameVr
Key
  Type
Ip
  String
192.170.179.0
Value
  Type
Vr
  String
vorbis-13@prsim
Key
  Type
Ip
  String
192.170.179.3
Value
  Type
Vr
  String
vorbis-13@prsim

...

Key
  Type
Vr
  String
default@sys1
Value
  Type
SaeId
  String
IOR:
000000000000003549444C3A736D67742E6A756E697065722E6E65742F7361652F53657276696365
41637469766174696F6E456E67696E653A312E30000000000000020000000000007800010200
0000000C31302E3232372E362E34330022610000000000226761726B6269742E6B616E6C61622E6A
6E70722E6E65742F736165504F412F5341450000000000200000000000008000000004A414300
000000010000001C0000000000010001000000010501000100010109000000010501000100000001
0000002C0000000000000001000000010000001C0000000000010001000000010501000100010109
0000000105010001

```

Meaning [Table 34 on page 205](#) describes the output fields for the **show nic data agent** command. Output fields are listed in the order in which they appear.

Table 34: Output Fields for show nic data agent

Field Name	Field Description
Component name	Name of an agent. Agent names have the format <code>/agents/ agent-name</code> .
Key	Data type and value of a NIC key. The value is the actual value of the NIC key, not the NIC value to which the key maps.
Value	Data type and value of the NIC value that maps to the associated NIC key.

Related Documentation

- [Viewing Statistics for NIC Agents \(SRC CLI\) on page 199](#)
- [Viewing Agents \(C-Web Interface\) on page 210](#)
- [Viewing Agent Statistics \(C-Web Interface\) on page 211](#)
- [Viewing Data for NIC Resolvers \(SRC CLI\) on page 201](#)

Troubleshooting NIC Data Resolution (SRC CLI)

Problem **Description:** The NIC does not resolve a request.

Solution Troubleshooting NIC data resolution is a complex task that requires a good understanding of how NIC operates, how it resolves resolution requests, and how the NIC configuration scenario that you are using performs resolutions.

This topic provides high-level troubleshooting information. For further assistance troubleshooting NIC operation and NIC resolutions, contact the Juniper Technical Support Center.

Troubleshoot NIC operation:

1. Make sure that the heap size configured for NIC is adequate and that the process is up:

```
user@host> show nic statistics process
```

Component Statistics

```
Component Name process
Heap in use    456194 bytes (87%)
Heap limit    524288 bytes
Threads       42
Up time       747848 seconds since Wed Jan 31 19:35:57 EST 2007
```

2. Determine whether there are any NIC resolution errors and whether NIC successfully completed any resolution requests:

```
user@host> show nic statistics host
```

Component Statistics

Component Name	/hosts
Number of Components Restart	0
Number of No Match Resolutions	0
Number of Resolution Errors	0
Number of Resolutions	0

3. Test the resolution process by using the **test nic resolve** command.

See *Configuring the NIC (SRC CLI)*.

If you are unsure whether NIC is resolving resolution requests, view data about those requests to see whether NIC is receiving data.

1. Verify that NIC is receiving data by running the **show nic data resolver** command.

See [“Viewing Data for NIC Resolvers \(SRC CLI\)” on page 201](#).

For each resolver, which is identified by a component name such as **/realms/login/C1**, the output should show a value, such as **default@sys1** for the key Vr, and the NIC value for that key such as the IOR that identifies an SAE.

2. If NIC is not receiving data, determine which agent or agents are not receiving data by running the **show nic data agent** command.

See [“Viewing Data for NIC Agents \(SRC CLI\)” on page 203](#).

3. Review your NIC configuration to make sure that NIC is configured correctly by running the **show** command for the NIC configuration scenario. For example:

```
[edit shared nic scenario OnePop]
user@host# show
```

- Related Documentation**
- *NIC Resolution Process Overview*
 - *NIC Configuration Scenarios*

CHAPTER 18

Monitoring the NIC (C-Web Interface)

- Viewing Hosts (C-Web Interface) on page 207
- Viewing Resolvers (C-Web Interface) on page 209
- Viewing Agents (C-Web Interface) on page 210

Viewing Hosts (C-Web Interface)

You can view statistics for hosts and the host process by:

- Viewing Host Statistics (C-Web Interface) on page 207
- Viewing Host Process Statistics (C-Web Interface) on page 208

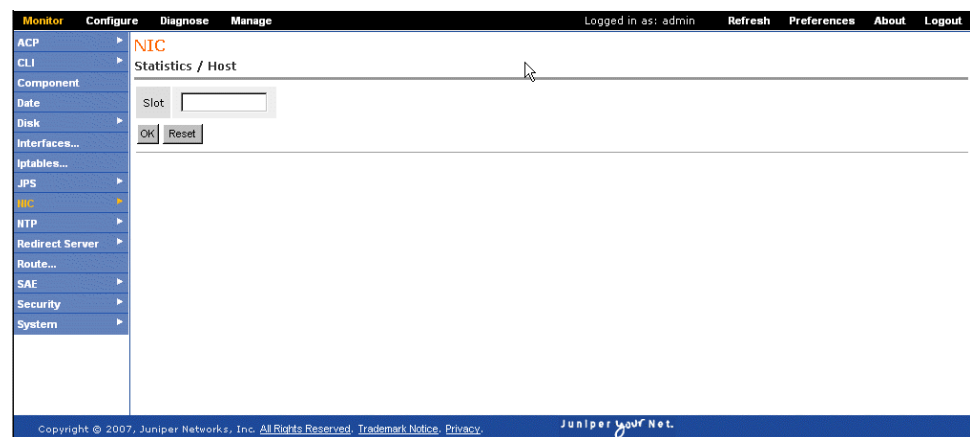
Viewing Host Statistics (C-Web Interface)

Purpose View NIC host statistics.

Action 1. Click **Monitor>NIC>Statistics>Host**.

The Statistics/Host pane appears.

Figure 38: C-Web Interface for Monitoring NIC Host Statistics



2. In the Slot box, enter the number of the slot for which you want to display host statistics.

3. Click **OK**.

The Statistics/Host pane displays the properties for the host.

- See Also**
- [Configuring the NIC \(C-Web Interface\)](#)
 - [Viewing Host Process Statistics \(C-Web Interface\) on page 208](#)
 - [Viewing Statistics for a NIC Host \(SRC CLI\) on page 197](#)

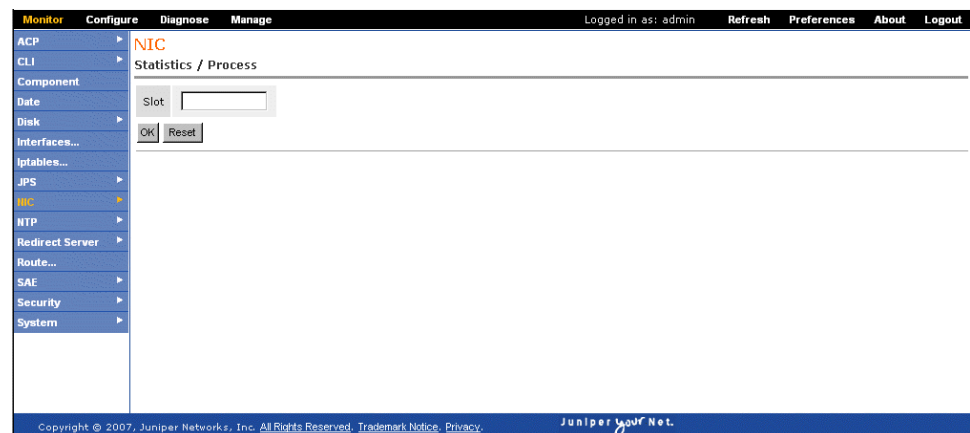
Viewing Host Process Statistics (C-Web Interface)

Purpose View NIC host process statistics.

- Action**
1. Click **Monitor>NIC>Statistics>Process**.

The Statistics/Process pane appears.

Figure 39: C-Web Interface for Monitoring NIC Host Process Statistics



2. In the Slot box, enter the number of the slot for which you want to display host process statistics.
3. Click **OK**.

The Statistics/Process pane displays the statistics for the host process.

- See Also**
- [Configuring the NIC \(C-Web Interface\)](#)
 - [Viewing Host Statistics \(C-Web Interface\) on page 207](#)
 - [Viewing Statistics for the NIC Process \(SRC CLI\) on page 196](#)

Viewing Resolvers (C-Web Interface)

You can view resolvers and monitor resolver statistics (C-Web Interface) by:

- [Viewing Resolvers \(C-Web Interface\) on page 209](#)
- [Viewing Resolver Statistics \(C-Web Interface\) on page 210](#)

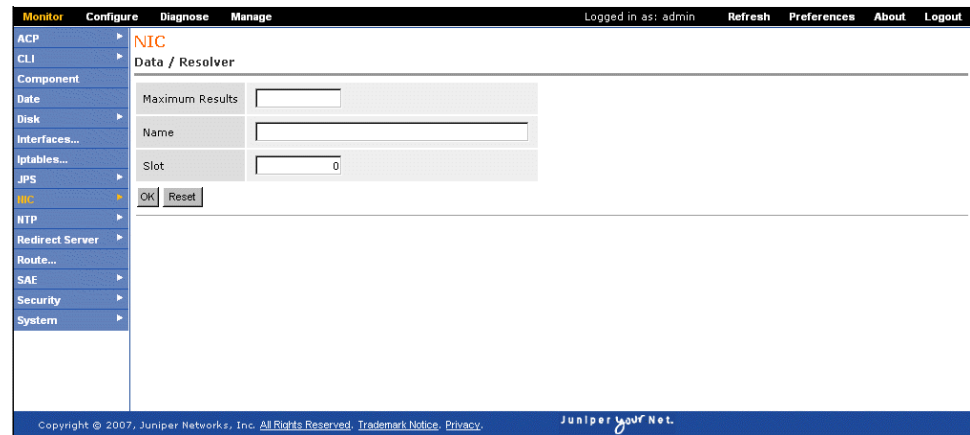
Viewing Resolvers (C-Web Interface)

Purpose View information about a resolver.

Action 1. Click **Monitor>NIC>Data>Resolver**.

The Data/Resolver pane appears.

Figure 40: C-Web Interface for Monitoring NIC Resolvers



2. In the Maximum Results box, enter the maximum number of results that you want to receive.
3. In the Name box, enter the name of the resolver for which you want to view data.
4. In the Slot box, enter the number of the slot for which you want to display resolver data.
5. Click **OK**.

The Data/Resolver pane displays the properties for the resolver.

- See Also**
- [Configuring the NIC \(C-Web Interface\)](#)
 - [Viewing Resolver Statistics \(C-Web Interface\) on page 210](#)
 - [Viewing Statistics for NIC Resolvers \(SRC CLI\) on page 198](#)
 - [Viewing Data for NIC Resolvers \(SRC CLI\) on page 201](#)

Viewing Resolver Statistics (C-Web Interface)

Purpose View statistics about resolvers.

Action 1. Click **Monitor>NIC>Statistics>Resolver**.

The Statistics/Resolver pane appears.

Figure 41: C-Web Interface for Monitoring NIC Resolver Statistics



2. In the Name box, enter the name of the resolver for which you want to view statistics.
3. In the Slot box, enter the number of the slot for which you want to display resolver statistics.
4. Click **OK**.

The Statistics/Resolver pane displays the statistics for the resolver.

- See Also**
- [Configuring the NIC \(C-Web Interface\)](#)
 - [Viewing Resolvers \(C-Web Interface\) on page 209](#)
 - [Viewing Statistics for NIC Resolvers \(SRC CLI\) on page 198](#)
 - [Viewing Data for NIC Resolvers \(SRC CLI\) on page 201](#)

Viewing Agents (C-Web Interface)

You can view agent properties or agent statistics with the C-Web interface by:

- [Viewing Agents \(C-Web Interface\) on page 210](#)
- [Viewing Agent Statistics \(C-Web Interface\) on page 211](#)

Viewing Agents (C-Web Interface)

Purpose View information about an agent.

Action 1. Click **Monitor>NIC>Data>Agent**.

The Data/Agent pane appears.

Figure 42: C-Web Interface for Monitoring NIC Agents

2. In the Maximum Results box, enter the maximum number of results that you want to receive.
3. In the Name box, enter the name of the agent for which you want to view data.
4. In the Slot box, enter the number of the slot for which you want to display agent data.
5. Click **OK**.

The Data/Agent pane displays the properties for the agent.

- See Also**
- [Configuring a NIC Scenario \(C-Web Interface\)](#)
 - [Viewing Data for NIC Agents \(SRC CLI\) on page 203](#)
 - [Viewing Agent Statistics \(C-Web Interface\) on page 211](#)
 - [Viewing Statistics for NIC Agents \(SRC CLI\) on page 199](#)

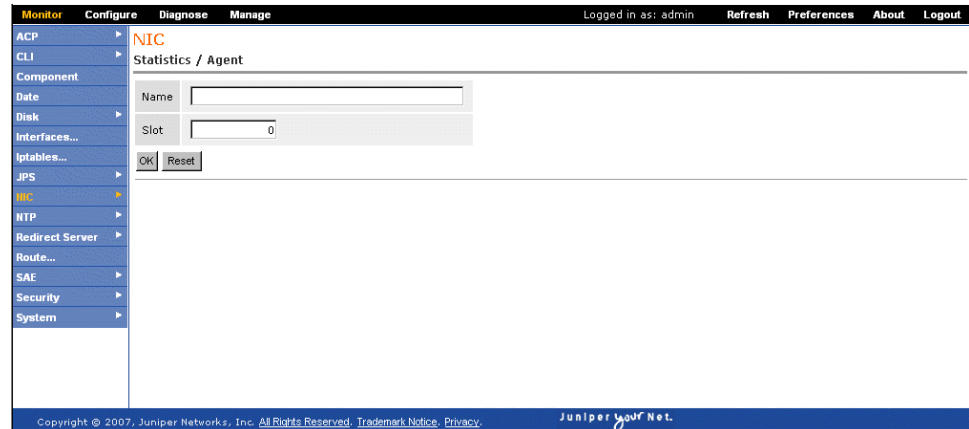
Viewing Agent Statistics (C-Web Interface)

Purpose View statistics for an agent.

Action 1. Click **Monitor>NIC>Statistics>Agent**.

The Statistics/Agent pane appears.

Figure 43: C-Web Interface for Monitoring NIC Agent Statistics



2. In the Name box, enter the name of the agent for which you want to view statistics.
3. In the Slot box, enter the number of the slot for which you want to display agent statistics.
4. Click **OK**.

The Statistics/Agent pane displays the properties for the agent.

- See Also**
- *Configuring a NIC Scenario (C-Web Interface)*
 - [Viewing Data for NIC Agents \(SRC CLI\) on page 203](#)
 - [Viewing Agents \(C-Web Interface\) on page 210](#)
 - [Viewing Statistics for NIC Agents \(SRC CLI\) on page 199](#)

CHAPTER 19

Monitoring NTP (SRC CLI)

- [Viewing NTP Peers \(SRC CLI\) on page 213](#)
- [Viewing Statistics for NTP \(SRC CLI\) on page 214](#)
- [Viewing Internal Variables for NTP \(SRC CLI\) on page 214](#)

Viewing NTP Peers (SRC CLI)

Purpose View a list of NTP peers with the SRC CLI.

Action user@host> **show ntp associations**

remote	local	st	poll	reach	delay	offset	disp
*myserver.jnpr.n	192.0.7.46	3	1024	377	0.00038	-0.000573	0.12178

Meaning [Table 35 on page 213](#) describes the output fields for the **show ntp associations** command. Output fields are listed in the approximate order in which they appear.

Table 35: Output Fields for show ntp associations command

remote	Address or name of the remote NTP peer
local	Address or name used by NTP on the local system
st	Stratum of the remote peer
poll	Polling interval, in seconds
reach	Reachability register, in octal
delay	Current estimated delay of the peer, in milliseconds
offset	Current estimated offset of the peer, in milliseconds
disp	Current estimated dispersion of the peer, in milliseconds

- Related Documentation**
- [Configuring an NTP Peer on a C Series Controller \(SRC CLI\)](#)
 - [Viewing Statistics for NTP \(SRC CLI\) on page 214](#)
 - [Viewing Internal Variables for NTP \(SRC CLI\) on page 214](#)
 - [Viewing NTP Peers \(C-Web Interface\) on page 217](#)

Viewing Statistics for NTP (SRC CLI)

Purpose View statistics for NTP with the SRC CLI.

Action user@host> show ntp statistics

```
time since restart: 2371617
time since reset: 2371617
packets received: 38765
packets processed: 2573
current version: 38761
previous version: 0
bad version: 0
access denied: 36188
bad length or format: 0
bad authentication: 0
rate exceeded: 0
```

- Related Documentation**
- [Configuring NTP on a C Series Controller](#)
 - [Viewing NTP Peers \(SRC CLI\) on page 213](#)
 - [Viewing Statistics for NTP \(C-Web Interface\) on page 218](#)
 - [Viewing NTP Status \(C-Web Interface\) on page 218](#)

Viewing Internal Variables for NTP (SRC CLI)

Purpose View information about internal variables for NTP with the SRC CLI:

Action user@host> show ntp status

```
system peer:      menemsha.jnpr.net
system peer mode: client
leap indicator:   00
stratum:         4
precision:       -20
root distance:    0.02245 s
root dispersion:  0.07689 s
reference ID:     [10.227.2.100]
reference time:   c922b152.86dd0529 Thu, Dec  7 2006 10:27:14.526
system flags:     auth monitor ntp kernel stats
jitter:          0.000183 s
stability:        1.728 ppm
broadcastdelay:   0.003998 s
authdelay:        0.000000 s
```

**Related
Documentation**

- [Viewing NTP Peers \(SRC CLI\) on page 213](#)
- [Viewing Statistics for NTP \(SRC CLI\) on page 214](#)
- [Viewing NTP Peers \(C-Web Interface\) on page 217](#)
- [Viewing Statistics for NTP \(C-Web Interface\) on page 218](#)
- [Viewing NTP Status \(C-Web Interface\) on page 218](#)

CHAPTER 20

Monitoring NTP (C-Web Interface)

- Viewing NTP Peers (C-Web Interface) on page 217
- Viewing Statistics for NTP (C-Web Interface) on page 218
- Viewing NTP Status (C-Web Interface) on page 218

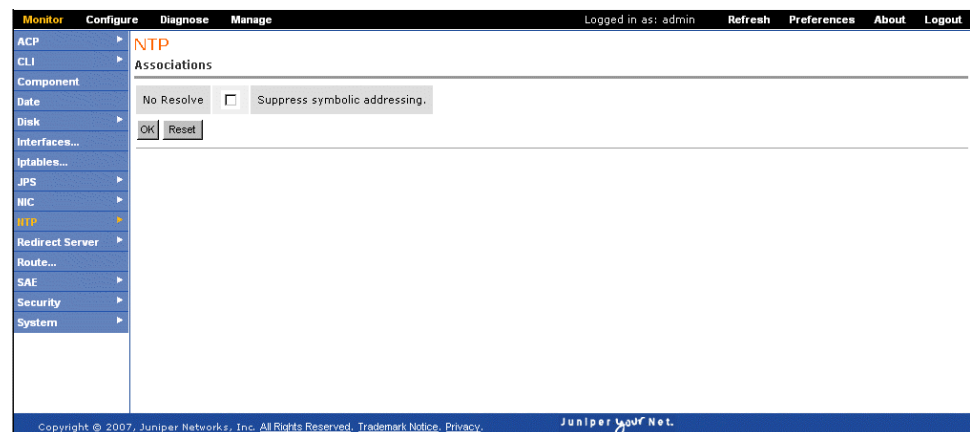
Viewing NTP Peers (C-Web Interface)

Purpose View a list of NTP peers.

Action 1. Click **Monitor>NTP>Associations**.

The Associations pane appears.

Figure 44: C-Web Interface for Monitoring NTP Peers



2. To suppress symbolic addressing, select the **No Resolve** box.
3. Click **OK**.

The Associations pane displays the list of NTP peers.

- Related Documentation**
- *Configuring an NTP Peer for a C Series Controller (C-Web Interface)*
 - Viewing NTP Peers (SRC CLI) on page 213
 - Viewing Statistics for NTP (C-Web Interface) on page 218

- [Viewing NTP Status \(C-Web Interface\) on page 218](#)

Viewing Statistics for NTP (C-Web Interface)

Purpose Display statistics for NTP.

Action 1. Click **Monitor>NTP>Statistics**.

The Statistics pane appears.

Figure 45: C-Web Interface for Monitoring NTP Statistics



2. To suppress symbolic addressing, select the **No Resolve** box.

3. Click **OK**.

The Statistics pane displays statistics for NTP.

Related Documentation

- [Specifying a Basic NTP Configuration on a C Series Controller \(C-Web Interface\)](#)
- [Viewing Statistics for NTP \(SRC CLI\) on page 214](#)
- [Viewing NTP Peers \(C-Web Interface\) on page 217](#)
- [Viewing NTP Status \(C-Web Interface\) on page 218](#)

Viewing NTP Status (C-Web Interface)

Purpose Display status for NTP.

Action 1. Click **Monitor>NTP>Status**.

The Status pane appears.

Figure 46: C-Web Interface for Monitoring NTP Status



2. To suppress symbolic addressing, select the **No Resolve** box.
3. Click **OK**.

The Status pane displays NTP status.

Related Documentation

- [Viewing NTP Peers \(SRC CLI\) on page 213](#)
- [Viewing Statistics for NTP \(SRC CLI\) on page 214](#)
- [Viewing Internal Variables for NTP \(SRC CLI\) on page 214](#)
- [Viewing NTP Peers \(C-Web Interface\) on page 217](#)
- [Viewing Statistics for NTP \(C-Web Interface\) on page 218](#)

CHAPTER 21

Monitoring Redirect Server (SRC CLI)

- [Viewing Statistics for the Redirect Server \(SRC CLI\) on page 221](#)
- [Viewing Statistics About Filtered Traffic \(SRC CLI\) on page 221](#)

Viewing Statistics for the Redirect Server (SRC CLI)

Purpose View statistics for redirect server.

Action user@host> `show redirect-server statistics`

```
Redirect Server
Uptime: 1270724.713 s
Accepted Requests: 25
Rejected Requests: 0
User limit leaky buckets: 0
User limits reached: 0
Global limits reached: 0
```

- Related Documentation**
- [Configuring the Redirect Server \(SRC CLI\)](#)
 - [Viewing Statistics About Filtered Traffic \(SRC CLI\) on page 221](#)
 - [Viewing Statistics for the Redirect Server \(C-Web Interface\) on page 223](#)
 - [Traffic Redirection Overview](#)

Viewing Statistics About Filtered Traffic (SRC CLI)

Purpose You can obtain information about the packets filtered on a C Series Controller by accessing statistics for the iptables Linux tool. You can also reset the counters for this tool.

Action To view information about packet filtering on a C Series Controller:

```
user@host> show iptables <nat | filter | mangle> <reset-counters>
```

Where:

- **nat**—Displays information for the nat table for the iptables tool. The nat table provides rules for rewriting packet addresses.
- **filter**—Displays information for the filter table for the iptables tool. The filter table provides rules for defining packet filters.
- **mangle**—Displays information for the mangle table for the iptables tool. The mangle table provides rules for adjusting packet options, such as quality of service.

For example:

```
user@host> show iptables
```

```
Chain INPUT (policy ACCEPT 25M packets, 9401M bytes)
pkts bytes target      prot opt in      out     source      destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source      destination

Chain OUTPUT (policy ACCEPT 24M packets, 4506M bytes)
pkts bytes target      prot opt in      out     source      destination
destinationreset-counters
```

To reset the values in the output for the **show iptables** command:

```
user@host> show iptables reset counters
```

Related Documentation

- *Configuring the Redirect Server (SRC CLI)*
- *Defining Traffic to Transmit to the Redirect Server (SRC CLI)*
- [Viewing Statistics for the Redirect Server \(SRC CLI\) on page 221](#)
- [Viewing Information for Filtered Traffic \(C-Web Interface\) on page 224](#)
- *Traffic Redirection Overview*

CHAPTER 22

Monitoring the Redirect Server and Filtered Traffic (C-Web Interface)

- Viewing Statistics for the Redirect Server (C-Web Interface) on page 223
- Viewing Information for Filtered Traffic (C-Web Interface) on page 224

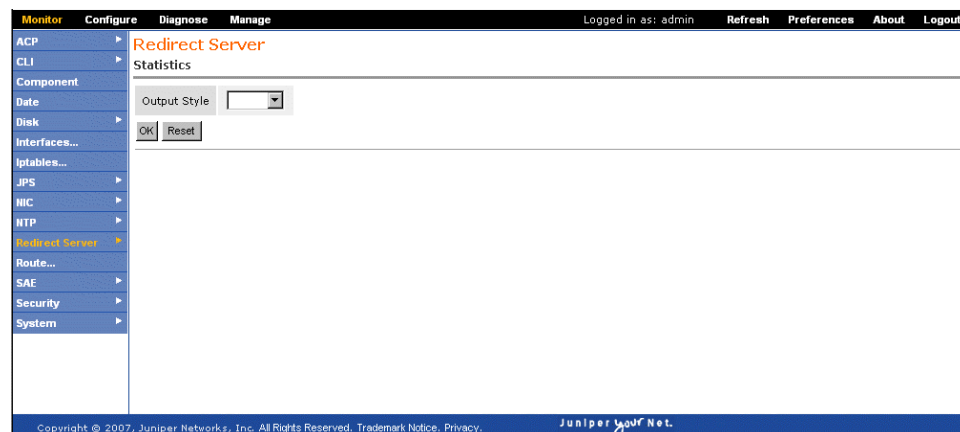
Viewing Statistics for the Redirect Server (C-Web Interface)

Purpose View statistics for the redirect server.

Action 1. Click **Monitor>Redirect Server>Statistics**.

The Statistics pane appears.

Figure 47: C-Web Interface for Monitoring Redirect Server Statistics



2. Select a style from the Output Style list.

3. Click **OK**.

The Statistics pane displays the redirect server statistics.

Related Documentation

- *Configuring General Properties for the Redirect Server (C-Web Interface)*
- *Configuring the Redirect Server (C-Web Interface)*

- [Viewing Statistics for the Redirect Server \(SRC CLI\) on page 221](#)
- [Viewing Information for Filtered Traffic \(C-Web Interface\) on page 224](#)
- [Traffic Redirection Overview](#)

Viewing Information for Filtered Traffic (C-Web Interface)

Purpose View information about filtered traffic with the **iptables Linux** tool when you are using C-Web to monitor the C Series Controller.

Action To view information about the filtered traffic:

1. Click **Monitor>Iptables**.

The Iptables pane appears.

Figure 48: C-Web Interface for Monitoring Filtered Traffic



2. Select the type of table that you want to display from the Table list:
 - nat—Displays information for the iptables NAT table
 - filter—Displays information for the iptables filter table
 - mangle—Displays information for the iptables mangle table
3. Select the **Reset Counters** check box to reset the counters of items in the output.
4. Click **OK**.

The Iptables pane displays information about filtered traffic.

Related Documentation

- [Defining Traffic to Transmit to the Redirect Server \(C-Web Interface\)](#)
- [Configuring the Redirect Server \(C-Web Interface\)](#)
- [Viewing Statistics About Filtered Traffic \(SRC CLI\) on page 221](#)
- [Viewing Statistics for the Redirect Server \(C-Web Interface\) on page 223](#)

- *Traffic Redirection Overview*

CHAPTER 23

Troubleshooting Network Connectivity (SRC CLI)

- [Commands to Troubleshoot Connections to Remote Hosts Overview on page 227](#)
- [Testing Connectivity to Remote Hosts \(SRC CLI\) on page 227](#)
- [Viewing the Route Information \(SRC CLI\) on page 228](#)
- [Viewing Routing Table Information \(SRC CLI\) on page 229](#)
- [Viewing Interface Information \(SRC CLI\) on page 229](#)

Commands to Troubleshoot Connections to Remote Hosts Overview

If you are troubleshooting problems with the SRC software that might be caused by connectivity problems to remote hosts, you can use the following commands:

- **ping**—Test connectivity to a remote host.
- **tracert**—Display the route from the local host to a remote host and back.
- **show interfaces**—Display information about system interfaces.
- **show route**—Display information from the system routing table.

Related Documentation

- [Testing Connectivity to Remote Hosts \(SRC CLI\) on page 227](#)
- [Viewing the Route Information \(SRC CLI\) on page 228](#)
- [Viewing Routing Table Information \(SRC CLI\) on page 229](#)
- [Viewing Interface Information \(SRC CLI\) on page 229](#)

Testing Connectivity to Remote Hosts (SRC CLI)

Purpose Test connectivity to a remote host.

Action user@host> ping

```
PING 10.227.7.45 (10.227.7.45) 56(84) bytes of data:
64 bytes from 10.227.7.45: icmp_seq=0 ttl=63 time=0.560 ms
64 bytes from 10.227.7.45: icmp_seq=1 ttl=63 time=0.613 ms
64 bytes from 10.227.7.45: icmp_seq=2 ttl=63 time=0.641 ms
64 bytes from 10.227.7.45: icmp_seq=3 ttl=63 time=0.653 ms
64 bytes from 10.227.7.45: icmp_seq=4 ttl=63 time=0.651 ms
64 bytes from 10.227.7.45: icmp_seq=5 ttl=63 time=0.418 ms
64 bytes from 10.227.7.45: icmp_seq=6 ttl=63 time=0.440 ms
64 bytes from 10.227.7.45: icmp_seq=7 ttl=63 time=0.454 ms
64 bytes from 10.227.7.45: icmp_seq=8 ttl=63 time=0.466 ms
64 bytes from 10.227.7.45: icmp_seq=9 ttl=63 time=0.478 ms
64 bytes from 10.227.7.45: icmp_seq=10 ttl=63 time=0.488 ms
```

Ctrl-C

```
--- 10.227.7.45 ping statistics ---
94 packets transmitted, 94 received, 0% packet loss, time 93038ms
rtt min/avg/max/mdev = 0.418/0.560/0.791/0.089 ms, pipe 2
```

For information about all the options for the **ping** command, see the *SRC PE CLI Command Reference*.

Related Documentation

- [Viewing the Route Information \(SRC CLI\) on page 228](#)
- [Viewing Routing Table Information \(SRC CLI\) on page 229](#)
- [Viewing Interface Information \(SRC CLI\) on page 229](#)
- [Commands to Troubleshoot Connections to Remote Hosts Overview on page 227](#)

Viewing the Route Information (SRC CLI)

Purpose You can use the **traceroute** command to get information about the hops between the local system and a remote host.

Action To view route information:

```
user@host> traceroute 192.2.7.48

traceroute to 192.2.7.48 (192.2.7.48), 30 hops max, 46 byte packets
 1 host (192.2.7.45) 3000.716 ms !H 3000.733 ms !H 3001.272 ms !H
```

For information about all the options for the **traceroute** command, see the *SRC PE CLI Command Reference*.

- Related Documentation**
- [Viewing Routing Table Information \(SRC CLI\) on page 229](#)
 - [Viewing Interface Information \(SRC CLI\) on page 229](#)
 - [Testing Connectivity to Remote Hosts \(SRC CLI\) on page 227](#)
 - [Commands to Troubleshoot Connections to Remote Hosts Overview on page 227](#)

Viewing Routing Table Information (SRC CLI)

Purpose You can display brief or detailed information about the route from the local system to a remote host.

Action To view brief route information:

```
user@host> show route
```

```
Kernel IP routing table
Destination      Gateway          Genmask          Flags   MSS Window  irtt Iface
192.2.2.0        ' ' ' ' ' ' ' ' * 255.255.255.0    U       0      0      0 eth0
default          src1ab1.mylab.  0.0.0.0          UG      0      0      0 eth0
```

To view detailed route information:

```
user@host> show route detail
```

```
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref  Use Iface MSS
Window irtt
192.2.2.0        ' ' ' ' ' ' ' ' * 255.255.255.0    U      0      0      0 eth0
' ' ' ' ' ' ' ' 0      0
default          src1ab1.mylab.  0.0.0.0          UG      0      0      0 eth0
' ' ' ' ' ' ' ' 0      0
```

The detailed output includes the additional Metric, Ref, and Use fields.

- Related Documentation**
- [Viewing Information About the Routing Table \(C-Web Interface\) on page 233](#)
 - [Viewing the Route Information \(SRC CLI\) on page 228](#)
 - [Viewing Interface Information \(SRC CLI\) on page 229](#)
 - [Testing Connectivity to Remote Hosts \(SRC CLI\) on page 227](#)
 - [Commands to Troubleshoot Connections to Remote Hosts Overview on page 227](#)

Viewing Interface Information (SRC CLI)

Purpose You can view information about all system interfaces, or about a specified interface.

Action To view information about all system interfaces:

```
user@host> show interfaces
```

```
eth0      Link encap:Ethernet  HWaddr 00:30:48:55:B6:FC
          inet addr:10.227.6.42  Bcast:10.227.6.255  Mask:255.255.255.0
          inet6 addr: fe80::230:48ff:fe55:b6fc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:482467 errors:0 dropped:0 overruns:0 frame:0
          TX packets:57573 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:38147790 (36.3 MiB)  TX bytes:4396018 (4.1 MiB)
          Base address:0xcc00  Memory:fc9c0000-fc9e0000
```

```
eth1      Link encap:Ethernet  HWaddr 00:30:48:55:B6:FD
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Base address:0xc800  Memory:fc9a0000-fc9c0000
```

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1946394 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1946394 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:260604464 (248.5 MiB)  TX bytes:260604464 (248.5 MiB)
```

```
lo:1      Link encap:Local Loopback
          inet addr:192.168.254.1  Mask:255.255.255.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
```

```
sit0      Link encap:IPv6-in-IPv4
          NOARP  MTU:1480  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

Related Documentation

- [Viewing Information About System Interfaces \(C-Web Interface\) on page 234](#)
- [Viewing the Route Information \(SRC CLI\) on page 228](#)

- [Viewing Routing Table Information \(SRC CLI\) on page 229](#)
- [Testing Connectivity to Remote Hosts \(SRC CLI\) on page 227](#)
- [Commands to Troubleshoot Connections to Remote Hosts Overview on page 227](#)

CHAPTER 24

Monitoring Network Connectivity (C-Web Interface)

- Viewing Information About the Routing Table (C-Web Interface) on page 233
- Viewing Information About System Interfaces (C-Web Interface) on page 234

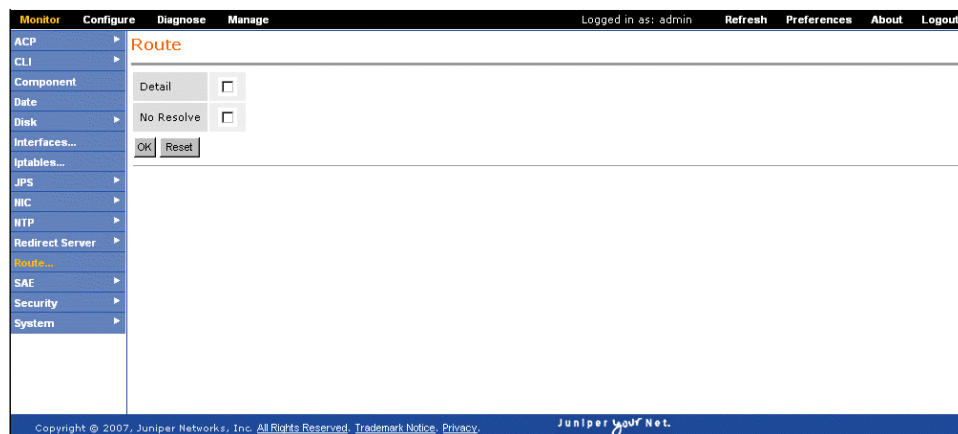
Viewing Information About the Routing Table (C-Web Interface)

Purpose View information about the route from the local system to a remote host.

Action 1. Click **Monitor>Route**.

The Route pane appears.

Figure 49: C-Web Interface for Monitoring Route Details



2. To suppress symbolic addressing, select the **No Resolve** box.
3. To display detailed output, select the **Detail** box.
4. Click **OK**.

The Route pane displays the information about the route.

Related Documentation

- Viewing Routing Table Information (SRC CLI) on page 229

- [Viewing Information About System Interfaces \(C-Web Interface\) on page 234](#)

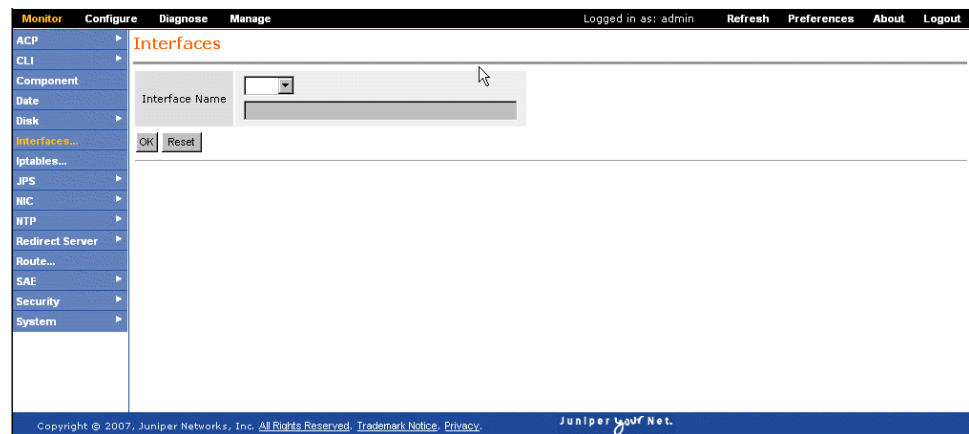
Viewing Information About System Interfaces (C-Web Interface)

Purpose View information about all system interfaces.

Action 1. Click **Monitor>Interfaces**.

The Interfaces pane appears.

Figure 50: C-Web Interface for Monitoring Interface Details



2. In the Interface name box, enter the name of the interface for which you want to view data.

3. Click **OK**.

The Interfaces pane displays the information about the interface.

Related Documentation

- [Viewing Interface Information \(SRC CLI\) on page 229](#)
- [Viewing Information About the Routing Table \(C-Web Interface\) on page 233](#)

Monitoring Activity for SRC Components

- [Monitoring Activity on C Series Controllers on page 235](#)
- [Collecting Data with the Activity Monitor \(SRC CLI\) on page 236](#)
- [Collecting Data with the Activity Monitor \(C-Web Interface\) on page 238](#)
- [Viewing Graphs \(C-Web Interface\) on page 238](#)
- [Viewing Graphs from a Webpage on page 239](#)

Monitoring Activity on C Series Controllers

The SRC software provides logging support and general statistics for SRC components. The Activity Monitor collects diagnostic information about the state of a component at a specific time and archives this information in one file.

You can collect the following information:

- Log files
- Configuration files
- stdout
- stderr
- Round-robin database (rrd) files generated by the Activity Monitor
- Output from system monitoring commands
- System log files, SAR data files, and other important log files in the system `/var/log` directory

The collected information is in a zipped tarball file that is named in the format **diagnostic-hostname-productname-YYMMDD-HHMMSS.tar.gz**—for example, **diagnostic-atlanta-C2000-20110926-184950.tar.gz**—and is found in the `/opt/UMC/activity/var/diagnostic/` directory. The tarball file contains the *diagnostic-info.log* file, which contains all the operations performed by the command and their success status. If an error occurred during an operation, the error message is logged.

The Activity Monitor can create graphs from the collected data to help determine the state of the SRC component for troubleshooting. You can view the graphs for the components during a specified time in the C-Web interface.

The generated graphs include data about the C Series Controller:

- CPU usage
- Load average
- Memory usage
- Interface traffic

The generated graphs for the SAE include the following data:

- Heap usage
- Service activity
- User activity
- Users and services

The generated graphs for the components include data generated from the MIBs.

- ACP—juniAcpHeapLimit, juniAcpHeapUsed, juniAcpIntfTrackingEvents, juniAcpIgnoredTrackingEvents, juniAcpCongestionPoints, juniAcpVirtualRouters, juniAcpCPUUpdateRcvd, juniAcpUserUpdateRcvd, juniAcpCPActiveUpdate, juniAcpUserActiveUpdate
- License server—juniSdxLicApplEntry
- NIC—juniNicHostHeapLimit, juniNicHostHeapUsed, juniNicHostResolutions, juniNicHostUnmatchedResolutions, juniNicHostResolutionErrors, juniNicHostResolutionTime
- SAE—juniSaeRouterCommonCurConn, juniSdxSaeUserLicenses

**Related
Documentation**

- [Collecting Data with the Activity Monitor \(SRC CLI\) on page 236](#)
- [Collecting Data with the Activity Monitor \(C-Web Interface\) on page 238](#)
- [Viewing Graphs \(C-Web Interface\) on page 238](#)
- [Viewing Graphs from a Webpage on page 239](#)

Collecting Data with the Activity Monitor (SRC CLI)

You can collect data with the Activity Monitor for specific components over a specified time and save them to a tar.gz file in the /opt/UMC/activity/var/diagnostic/* directory. You can view the exact file name and path after you execute the **request support information** command. Before you perform data collection with the Activity Monitor, make sure the filter for the specific components is enabled.

To perform data collection with the Activity Monitor:

- `user@host> request support information`

Some of the information retrieved includes:

- System log messages from the `/var/log/messages/*` directory.
- The configuration in text format, XML format, and set format.
- The hostname in the name of the diagnostic file.

To perform data collection for specific components:

- `user@host> request support information component`

where ***component*** is one of the following:

- acp—SRC Admission Control Plug-In
- activity—Activity Monitor
- agent—SNMP agent
- appsvr—Application server
- cli—SRC CLI
- diameter—Diameter application
- dsa—Dynamic Service Activator
- extsubmon—External Subscriber Monitor
- ims—IP multimedia subsystem
- jdb—Juniper Networks database
- licSvr—License server
- nic—Network information collector
- redir—Redirect server
- sae—SAE
- webadm—C-Web interface

To perform data collection for a specified number of days:

- `user@host> request support information days`

where ***days*** is in the range of 1–36500.

Related Documentation

- [Before You Load a Configuration](#)
- [Viewing Graphs \(C-Web Interface\) on page 238](#)
- [Viewing Graphs from a Webpage on page 239](#)
- [Monitoring Activity on C Series Controllers on page 235](#)

Collecting Data with the Activity Monitor (C-Web Interface)

You can collect data with the Activity Monitor for specific components over a specified time. Before you configure data collection for the Activity Monitor, make sure the Activity Monitor (activity), CLI (cli), and C-Web interface (webadm) components are enabled.

To perform data collection with the Activity Monitor:

1. Click **Manage>Request>Support>Information**.
The Support Information pane appears.
2. From the Components list, select the components you want to monitor, and click **OK**.
3. (Optional) Enter the number of days for which you want to collect data, and click **OK**.

Related Documentation

- [Viewing Graphs \(C-Web Interface\) on page 238](#)
- [Viewing Graphs from a Webpage on page 239](#)
- [Monitoring Activity on C Series Controllers on page 235](#)

Viewing Graphs (C-Web Interface)

You can display graphs for components for which the Activity Monitor has collected data.

To display graphs from the Activity Monitor with the C-Web interface:

1. Click **Graphs**.
2. In the side pane, select the component and the graph that you want to display.
The pane for selecting the time period displayed by the graph appears.
3. Select one of the preset values or enter the time range in the From and To boxes, and click **OK**.
The graphs appear.

Related Documentation

- [Collecting Data with the Activity Monitor \(C-Web Interface\) on page 238](#)
- [Viewing Graphs from a Webpage on page 239](#)
- [Monitoring Activity on C Series Controllers on page 235](#)

Viewing Graphs from a Webpage

You can display graphs for components for which the Activity Monitor has collected data from a webpage. Before you display these graphs, make sure the Activity Monitor (activity) and C-Web interface (webadm) components are enabled. For more secure displays, configure the C-Web interface to use HTTPS and use POST requests.

- [Viewing Graphs for a Preset Time Period from a Webpage on page 239](#)
- [Viewing Graphs for Specified Time Periods from a Webpage on page 240](#)

Viewing Graphs for a Preset Time Period from a Webpage

To display graphs with preset time periods from the Activity Monitor from a webpage:

`http://ip-address/graph?&id=username&pw=password&name=graph-name&time=time-period`

where

- *ip-address*—IP address of the C Series Controller
- *username*—Username used to log in to the C Series Controller
- *password*—Password used to log in to the C Series Controller
- *graph-name*—Name of graph to display in the format `<component>-<graph>`, where `<graph>` is the name of the graph as specified in the C-Web interface in all lowercase letters with hyphens separating words
- *time-period*—Period of time that data was collected for display in a graph in the format `<number><units>`

The `<number>` is the number of `<units>`, which are specified as one of the following values:

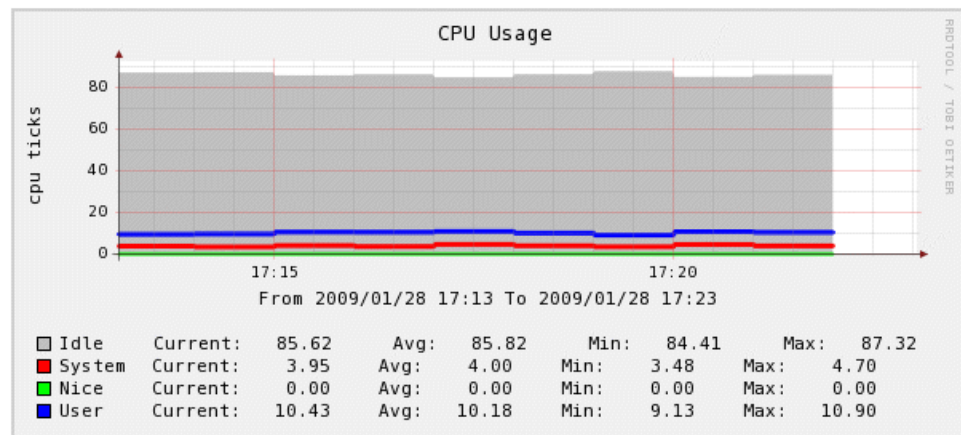
- m—minutes
- h—hours
- d—days
- w—weeks
- M—months
- y—years

For example, to view the CPU graph for the System component for the past 10 minutes on the C Series Controller called c2000 for the user admin:

`http://c2000/graph?&id=admin&pw=secret&name=system-cpu&time=10m`

The CPU Usage graph appears.

Figure 51: Sample CPU Usage Graph



Viewing Graphs for Specified Time Periods from a Webpage

To display graphs for specified time periods from the Activity Monitor from a webpage:

`http://ip-address/graph?&id=username&pw=password&name=graph-name&start=date-time&end=date-time`

where

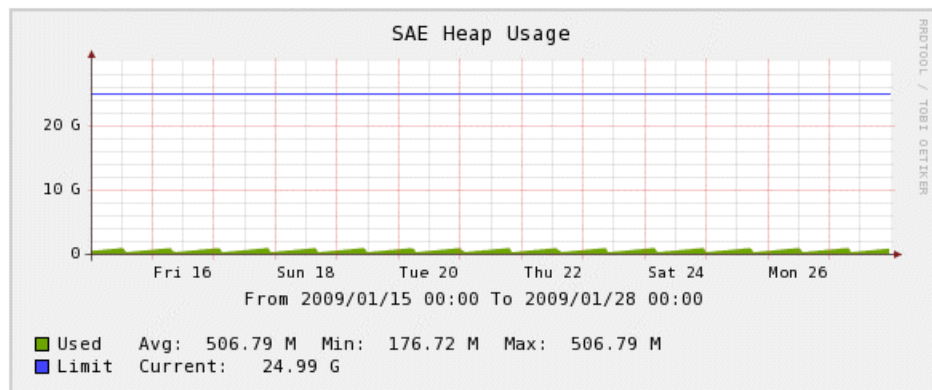
- *ip-address*—IP address of the C Series Controller
- *username*—Username used to log in to the C Series Controller
- *password*—Password used to log in to the C Series Controller
- *graph-name*—Name of graph to display in the format `<component>-<graph>`, where `<graph>` is the name of the graph as specified in the C-Web interface in all lowercase letters with hyphens separating words
- *date-time*—Date and time that data was collected for display in a graph in the format `yyyyMMddHHmm`, where:
 - *yyyy*—year
 - *MM*—month
 - *dd*—day
 - *HH*—hour
 - *mm*—minute

For example, to view the heap usage graph for the SAE component from January 15 to January 28 on the C Series Controller called c2000 for the user admin:

`http://c2000/graph?&id=admin&pw=secret&name=sae-heap&start=200901150000&end=200901280000`

The SAE Heap Usage graph appears.

Figure 52: Sample SAE Heap Usage Graph



Related Documentation

- [Collecting Data with the Activity Monitor \(SRC CLI\) on page 236](#)
- [Collecting Data with the Activity Monitor \(C-Web Interface\) on page 238](#)
- [Viewing Graphs \(C-Web Interface\) on page 238](#)
- [Monitoring Activity on C Series Controllers on page 235](#)

