Chapter 11

Understanding Traps

This chapter describes the trap information for performance and event traps and provides alarm state information. Topics include:

For information about using the SRC CLI that runs on Solaris platforms and the C-series controllers to configure traps, see *Chapter 9, Configuring the SNMP Traps with the SRC CLI*.

For information about using configuration applications to configure traps on a Solaris platform, see *Chapter 10, Configuring the SNMP Traps on a Solaris Platform*.

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 6 describes the symbols used in the performance traps tables.

Table 6: 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

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.

Decoding 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.

Tasks to decode trap numbers are:

- Decoding Trap Numbers for Raised Trap Actions on page 69
- Decoding Trap Numbers for Clear Trap Actions on page 69

You can access the MIBs on the Juniper Web site at

http://www.juniper.net/techpubs/software/management/sdx

Decoding Trap Numbers for Raised Trap Actions

To decode a trap number for raised trap actions:

- Use the following equation:

  Trap number = Trap ID * 10 + 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.

Decoding Trap Numbers for Clear Trap Actions

To decode a trap number for clear trap actions:

- Use the following equation:

  Trap number = 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.

SAE Performance Traps

Table 7 lists the performance traps for the SAE.

Table 7: Performance Traps–SAE

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
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
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

Table 7: Performance Traps–SAE (continued)

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/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

Accounting Performance Traps

Table 8 lists the performance traps for accounting.

Table 8: Performance Traps–Accounting

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
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
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

Table 8: Performance Traps–Accounting (continued)

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
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

Authentication Performance Traps

Table 9 lists the performance traps for authentication.

Table 9: Performance Traps–Authentication

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
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

Table 9: Performance Traps–Authentication (continued)

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
saeAuthMalformedAccessResponses	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
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

NIC Performance Traps

Table 10 lists the performance traps for NIC.

Table 10: Performance Traps–NIC

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
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

Router Driver Performance Traps

Table 11 lists the performance traps for router drivers.

Table 11: Performance Traps–Router Drivers

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
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
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

Table 11: Performance Traps–Router Drivers (continued)

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
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

Workflow Performance Traps

Table 12 lists the performance traps for workflows.

Table 12: Performance Traps–Workflow

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
wkfInstanceFileSize	90	$S:Workflow:The instance data allocated for each active workflow is $Dk. This $L the threshold of $Tk.:$A	7	5	2	60	AV
wkfEventFileSize	91	$S:Workflow:The pending events filesize is $Dk. This $L the threshold of $Tk.:$A	500	250	100	60	AV
wkfReportFileSize	92	$S:Workflow:The pending reports filesize is $Dk. This $L the threshold of $Tk.:$A	250	125	50	60	AV
wkfPersistentFileSize	93	$S:Workflow:The persistent storage allocated for each active workflow is $Dk. This $L the threshold of $Tk.:$A	70	50	20	60	AV
wkfCancelledWorkflows	94	$S:Workflow:During the last $Ps, $D workflows have been cancelled. This $L the threshold of $T cancelled workflows.:$A	100	50	10	60	R
wkfPendingEvents	95	$S:Workflow:The number of pending events is $D. This $L the threshold of $T pending events.:$A	1000	500	100	60	AV
wkfActiveWorkflows	96	$S:Workflow:The number of active workflows is $D. This $L the threshold of $T active workflows.:$A	1000	500	100	60	AV
wkfRunningWorkflows	97	$S:Workflow:The number of running workflows is $D. This $L the threshold of $T workflows.:$A	1000	500	100	60	AV

System Management Performance Traps

Table 13 lists the performance traps for system management event.

Table 13: Performance Traps–System Management Event

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
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

Policy Engine Performance Traps

Table 14 lists the performance traps for policy engine.

Table 14: Performance Traps–Policy Engine

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
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
penAvgICMModProcTime	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
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

SRC Redirector Performance Traps

Table 15 lists the performance traps for SRC redirector.

Table 15: Performance Traps–SRC Redirector

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
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

SRC-ACP Performance Traps

Table 16 lists the performance traps for the SRC-Admission Control Plug-In (SRC-ACP) application.

Table 16: Performance Traps–SRC-ACP

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

JPS Performance Traps

Table 17 lists the performance traps for the Juniper Policy Server (JPS).

Table 17: Performance Traps–JPS

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
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
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

Event Traps

Table 18 lists the event traps.

Table 18: 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
routerConnClosed	211	When juniSaeRouterUseFailOver is FALSE: ■ INFORMATION:SAE Router Driver:The router connection to $juniSaeRouterClientId has been closed.:RAISE When juniSaeRouterUseFailOver is TRUE: ■ 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	When the trap is raised, the text displayed is: ■ 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 When the trap is cleared, the text displayed is: ■ 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
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
acpSyncCompleted	290	INFORMATION:ACP State Sync:ACP finished state sync with SAE for $juniAcpVirtualRouterName.:RAISE

Table 18: Event Traps (continued)

Trap Event	Trap ID	Text Displayed
acpRedundStateSwitched	291	INFORMATION:ACP Host:The redundancy state of the ACP Host has switched to $juniAcpRedundState.:RAISE
jpsAmConnUp	260	INFORMATION:JPS:A new application manager connection was established.:RAISE
jpsAmConnDown	261	INFORMATION:JPS:The application manager connection went down.:RAISE
jpsCmtsConnUp	262	INFORMATION:JPS:A new CMTS connection was established.:RAISE
jpsCmtsConnDown	263	INFORMATION:JPS:A CMTS connection went down.:RAISE
systemOperatingFailure	300	When the trap is raised, the text displayed is: ■ INFORMATION:System:hardware failure is found with $juniSdxOperatingSensor on system $juniSdxOperatingLocation:RAISE When the trap is cleared, the text displayed is: ■ INFORMATION:System:hardware failure with $juniSdxOperatingSensor on system $juniSdxOperatingLocation is cleared:CLEAR
diskFailure	301	When the trap is raised, the text displayed is: ■ INFORMATION:System:disk failure is found:RAISE When the trap is cleared, text displayed is: ■ INFORMATION:System:disk failure is cleared:CLEAR

Alarm State Transitions

Table 19 lists the alarm state transitions.

Table 19: Alarm State Transitions

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