CHAPTER 2

Audit Troubleshooting

Revised: July 22, 2009, OL-8000-32

Introduction

This chapter provides the information needed to monitor and troubleshoot Audit events and alarms. This chapter is divided into the following sections:

- Audit Events and Alarms – Provides a brief overview of each Audit event and alarm.
- Monitoring Audit Events – Provides the information needed to monitor and correct Audit events.
- Troubleshooting Audit Alarms – Provides the information needed to troubleshoot and correct Audit alarms.

Audit Events and Alarms

This section provides a brief overview of the Audit events and alarms for the Cisco BTS 10200 Softswitch in numerical order. Table 2-1 lists all of the audit events and alarms by severity.

Note Click the Audit message number in Table 2-1 to display information about the event or alarm.

Table 2-1 Audit Events and Alarms by Severity

CRITICAL	MAJOR	MINOR	WARNING	INFO
AUDIT (5)	AUDIT (6)	AUDIT (7)	AUDIT (3)	AUDIT (1)
AUDIT (11)	AUDIT (12)	AUDIT (13)	AUDIT (4)	AUDIT (2)
AUDIT (18)	AUDIT (17)	AUDIT (16)	AUDIT (8)	AUDIT (10)
	AUDIT (20)		AUDIT (9)	AUDIT (14)
			AUDIT (15)	
			AUDIT (19)	

AUDIT (1)

For additional information, refer to the "Test Report - Audit (1)" section on page 2-12.

DESCRIPTION	Test Report
SEVERITY	Information (INFO)
THRESHOLD	100
THROTTLE	0
PRIMARY CAUSE	This event is used for testing the new "Audit" category.
PRIMARY ACTION	No action is necessary.

AUDIT (2)

For additional information, refer to the "Start or Stop of Signaling System 7 - Circuit Identification Code Audit - Audit (2)" section on page 2-12.

DESCRIPTION	Start or Stop of Signaling System 7-Circuit Identification Code Audit
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Type of Audit - STRING [64]
PRIMARY CAUSE	Signaling System 7 (SS7) circuit identification code (CIC) audit has started or stopped.
PRIMARY ACTION	No action required - normal operation.

AUDIT (3)

To monitor and correct the cause of the event, refer to the "Signaling System 7 Circuit Identification Code Audit Terminated Before Successful Completion - Audit (3)" section on page 2-13.

DESCRIPTION	Signaling System 7 Circuit Identification Code Audit Terminated Before Successful Completion
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Type of Audit - STRING [64]
PRIMARY CAUSE	A higher priority SS7 CIC audit interrupted and terminated a lower priority SS7 CIC audit.
PRIMARY ACTION	Do not schedule an SS7 remote termination audit to occur while a periodic SS7 local termination audit is executing.

AUDIT (4)

To monitor and correct the cause of the event, refer to the "Call Exceeds a Long-Duration Threshold - Audit (4)" section on page 2-13

DESCRIPTION	Call Exceeds a Long-Duration Threshold
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Trunk group number - TWO_BYTES Trunk member number - TWO_BYTES Current long-duration threshold - TWO_BYTES
PRIMARY CAUSE	Call exceeds current system long-duration threshold.
PRIMARY ACTION	If there is reason to believe the call is no longer valid, release the associated trunk facility.

AUDIT (5)

To troubleshoot and correct the cause of the alarm, refer to the "Critical Internal Audit Failure - Audit (5)" section on page 2-17.

DESCRIPTION	Critical Internal Audit Failure
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Failure Details - STRING [220] Probable Causes - STRING [80] Corrective Actions - STRING [80]
PRIMARY CAUSE	See data field.
PRIMARY ACTION	See data field.

AUDIT (6)

To troubleshoot and correct the cause of the alarm, refer to the "Major Internal Audit Failure - Audit (6)" section on page 2-17.

DESCRIPTION	Major Internal Audit Failure
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Failure Details - STRING [220] Probable Causes - STRING [80] Corrective Actions - STRING [80]
PRIMARY CAUSE	See data field.
PRIMARY ACTION	See data field.

AUDIT (7)

To troubleshoot and correct the cause of the alarm, refer to the "Minor Internal Audit Failure - Audit (7)" section on page 2-17.

DESCRIPTION	Minor Internal Audit Failure
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Failure Details - STRING [220] Probable Causes - STRING [80] Corrective Actions - STRING [80]
PRIMARY CAUSE	See data field.
PRIMARY ACTION	See data field.

AUDIT (8)

To monitor and correct the cause of the event, refer to the "Warning From Internal Audit - Audit (8)" section on page 2-14.

DESCRIPTION	Warning From Internal Audit
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Failure Details - STRING [220] Probable Causes - STRING [80] Corrective Actions - STRING [80]
PRIMARY CAUSE	See data field.
PRIMARY ACTION	See data field.

AUDIT (9)

To monitor and correct the cause of the event, refer to the "Softswitch Audit SIP CCB Release - Audit (9)" section on page 2-14.

DESCRIPTION	Softswitch Audit SIP CCB Release
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	AORID - STRING [64] TGID - TWO_BYTES
PRIMARY CAUSE	One side of the BTS 10200 was inactive.
PRIMARY ACTION	The SIA determines that a network error or DNS error occurred.
SECONDARY CAUSE	A software error has occurred.
SECONDARY ACTION	Contact the BTS 10200 engineer. Contact Cisco TAC.

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

AUDIT (10)

For additional information, refer to the "Memory Audit Complete Status - Audit (10)" section on page 2-14.

DESCRIPTION	Memory Audit Complete Status
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Audit Type and Total Freed Count - STRING [256]
PRIMARY CAUSE	A SIP memory audit pass has been completed.
PRIMARY ACTION	Check to see if any call blocks are freed as a result of the audit. An investigation for root cause may be useful.

AUDIT (11)

To troubleshoot and correct the cause of the alarm, refer to the "Critical Network Time Protocol Service Failure - Audit (11)" section on page 2-18.

DESCRIPTION	Critical Network Time Protocol Service Failure
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Failure Details - STRING [220] Probable Causes - STRING [80] Corrective Actions - STRING [80]
PRIMARY CAUSE	See data field.
PRIMARY ACTION	See data field.

AUDIT (12)

To troubleshoot and correct the cause of the alarm, refer to the "Major Network Time Protocol Service Failure - Audit (12)" section on page 2-18.

DESCRIPTION	Major Network Time Protocol Service Failure
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Failure Details - STRING [220] Probable Causes - STRING [80] Corrective Actions - STRING [80]
PRIMARY CAUSE	See data field.
PRIMARY ACTION	See data field.

AUDIT (13)

To troubleshoot and correct the cause of the alarm, refer to the "Minor Network Time Protocol Service Failure - Audit (13)" section on page 2-18.

DESCRIPTION	Minor Network Time Protocol Service Failure
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Failure Details - STRING [220] Probable Causes - STRING [80] Corrective Actions - STRING [80]
PRIMARY CAUSE	See data field.
PRIMARY ACTION	See data field.

AUDIT (14)

To monitor and correct the cause of the event, refer to the "Network Time Protocol Service Warning - Audit (14)" section on page 2-15.

DESCRIPTION	Network Time Protocol Service Warning
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Failure Details - STRING [220] Probable Causes - STRING [80] Corrective Actions - STRING [80]
PRIMARY CAUSE	See data field.
PRIMARY ACTION	See data field.

AUDIT (15)

To troubleshoot and correct the cause of the alarm, refer to the "Critical Index Shared Memory Error - Audit (15)" section on page 2-18.

DESCRIPTION	Critical Index Shared Memory Error
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Failure Details - STRING [220] Probable Causes - STRING [80] Corrective Actions - STRING [80]
PRIMARY CAUSE	See data field.
PRIMARY ACTION	See data field.

AUDIT (16)

To troubleshoot and correct the cause of the alarm, refer to the "Process Heap Memory Usage Exceeds Minor Threshold Level - Audit (16)" section on page 2-18.

DESCRIPTION	Process Heap Memory Usage Exceeds Minor Threshold Level
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Process Name - STRING [10] Heap Size in KB - FOUR_BYTES Heap Limit in KB - FOUR_BYTES Heap Usage Percentage - FOUR_BYTES Threshold Level Percentage - FOUR_BYTES
PRIMARY CAUSE	Increase in heap usage due to high call traffic or maintenance operation.
PRIMARY ACTION	Monitor heap usage frequently and see whether it is approaching major threshold level.

AUDIT (17)

To troubleshoot and correct the cause of the alarm, refer to the "Process Heap Memory Usage Exceeds Major Threshold Level - Audit (17)" section on page 2-18.

DESCRIPTION	Process Heap Memory Usage Exceeds Major Threshold Level
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Process Name - STRING [10] Heap Size in KB - FOUR_BYTES Heap Limit in KB - FOUR_BYTES Heap Usage Percentage - FOUR_BYTES Threshold Level Percentage - FOUR_BYTES
PRIMARY CAUSE	Increase in heap usage due to high call traffic or maintenance operation or software problem.
PRIMARY ACTION	Schedule a switchover during maintenance window.

AUDIT (18)

To troubleshoot and correct the cause of the alarm, refer to the "Process Heap Memory Usage Exceeds Critical Threshold Level - Audit (18)" section on page 2-19.

DESCRIPTION	Process Heap Memory Usage Exceeds Critical Threshold Level
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Process Name - STRING [10] Heap Size in KB - FOUR_BYTES Heap Limit in KB - FOUR_BYTES Heap Usage Percentage - FOUR_BYTES Threshold Level Percentage - FOUR_BYTES
PRIMARY CAUSE	Increase in heap usage due to high call traffic or maintenance operation or software problem.
PRIMARY ACTION	Schedule a switchover during maintenance window as soon as possible.

AUDIT (19)

To monitor and correct the cause of the event, refer to the "Recovered Memory of Stale Call - Audit (19)" section on page 2-16.

DESCRIPTION	Recovered Memory of Stale Call
SEVERITY	WARNING
THRESHOLD	20
THROTTLE	0
DATAWORDS	Stale Memory Release Info - STRING [128]
PRIMARY CAUSE	Loss of communication with originating or terminating side.
PRIMARY ACTION	Check if adjacent network element is up and having proper communication link with softswitch.
SECONDARY CAUSE	Adjacent network device protocol error.
SECONDARY ACTION	Check the adjacent network device protocol compatibility.
TERNARY CAUSE	An internal software error has occurred.
TERNARY ACTION	Contact Cisco Support. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

AUDIT (20)

To troubleshoot and correct the cause of the alarm, refer to the "Audit Found Lost Call Data Record - Audit (20)" section on page 2-19.

DESCRIPTION	Audit Found Lost Call Data Record
SEVERITY	MAJOR
THRESHOLD	20
THROTTLE	0
DATAWORDS	Error Text - STRING [200]
PRIMARY CAUSE	Software error - however, the orphaned records are recovered on detection 2d.
PRIMARY ACTION	Contact Cisco Support (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Monitoring Audit Events

This section provides the information needed to monitor and correct Audit events. Table 2-2 lists all Audit events in numerical order and provides cross reference to each subsection in this section.

Table 2-2 Cisco BTS 10200 Softswitch Audit Events

Event Type	Event Name	Event Severity
AUDIT(1)	Test Report - Audit (1)	INFO
AUDIT(2)	Start or Stop of Signaling System 7 - Circuit Identification Code Audit - Audit (2)	INFO
AUDIT(3)	Signaling System 7 Circuit Identification Code Audit Terminated Before Successful Completion - Audit (3)	WARNING
AUDIT(4)	Call Exceeds a Long-Duration Threshold - Audit (4)	WARNING
AUDIT(5)	Critical Internal Audit Failure - Audit (5)	CRITICAL
AUDIT(6)	Major Internal Audit Failure - Audit (6)	MAJOR
AUDIT(7)	Minor Internal Audit Failure - Audit (7)	MINOR
AUDIT(8)	Warning From Internal Audit - Audit (8)	WARNING
AUDIT(9)	Softswitch Audit SIP CCB Release - Audit (9)	WARNING
AUDIT(10)	Memory Audit Complete Status - Audit (10)	INFO
AUDIT(11)	Critical Network Time Protocol Service Failure - Audit (11)	CRITICAL
AUDIT(12)	Major Network Time Protocol Service Failure - Audit (12)	MAJOR
AUDIT(13)	Minor Network Time Protocol Service Failure - Audit (13)	MINOR
AUDIT(14)	Network Time Protocol Service Warning - Audit (14)	WARNING
AUDIT(15)	Critical Index Shared Memory Error - Audit (15)	CRITICAL
AUDIT(16)	Process Heap Memory Usage Exceeds Minor Threshold Level - Audit (16)	MINOR
AUDIT(17)	Process Heap Memory Usage Exceeds Major Threshold Level - Audit (17)	MAJOR
AUDIT(18)	Process Heap Memory Usage Exceeds Critical Threshold Level - Audit (18)	CRITICAL
AUDIT(19)	Recovered Memory of Stale Call - Audit (19)	WARNING
AUDIT(20)	Audit Found Lost Call Data Record - Audit (20)	MAJOR

Test Report - Audit (1)

The Test Report event is used for testing the audit event category. The event is informational and no further action is required.

Start or Stop of Signaling System 7 - Circuit Identification Code Audit - Audit (2)

The Start or Stop of Signaling System 7 - Circuit Identification Code Audit event occurs as part of normal Cisco BTS 10200 Softswitch operation. The event is informational and no further action is required.

Signaling System 7 Circuit Identification Code Audit Terminated Before Successful Completion - Audit (3)

The Signaling System 7 Circuit Identification Code Audit Terminated Before Successful Completion event serves as a warning that a higher priority SS7 CIC audit has interrupted and terminated a lower priority SS7 CIC audit. To control the occurrence of this event an SS7 remote termination audit should not be scheduled to occur while a periodic SS7 local termination audit is executing.

Call Exceeds a Long-Duration Threshold - Audit (4)

The Call Exceeds a Long-Duration Threshold event serves as a warning that a call has exceeded the current the Cisco BTS 10200 Softswitch system long-duration threshold. If there is reason to believe the call is no longer valid, the associated trunk facility should be released.

To check the current threshold setting for Long Duration calls, proceed as follows:

Step 1 As root user from the Call Agent (CA), execute the following command:

```
# grep LongDuration /opt/OptiCall/`ls /opt/OptiCall | grep CA`/bin/platform.cfg
```

Step 2 Review the command results.

Example results:

```
Args=-ems_pri_dn blg-asys07EMS.mssol.cisco.com -ems_sec_dn blg-asys07EMS.mssol.cisco.com
-port 15260
-QCheckInterval1 1000 -QCheckInterval2 4500 -RecordGenTime 00:00:00 -LongDurationAllowance
1440
-QCheckInterval3 60 -MyCaBillingDn blg-asys07CA.mssol.cisco.com
```

Note Following a platform start, the billing system will wait until the present time (current time on the call agent) is equal to RecordGenTime before auditing for Long Duration Calls. After the initial audit, the billing system will perform a Long Duration Call audit every LongDurationAllowance minutes. During an audit, the billing system will generate a Long Duration CDR for calls that have been active for LongDurationAllowance minutes.

Critical Internal Audit Failure - Audit (5)

The Critical Internal Audit Failure alarm (critical) indicates that a critical internal audit failure has occurred. To troubleshoot and correct the cause of the Critical Internal Audit Failure alarm, refer to the "Critical Internal Audit Failure - Audit (5)" section on page 2-17.

Major Internal Audit Failure - Audit (6)

The Major Internal Audit Failure alarm (major) indicates that a major internal audit failure has occurred. To troubleshoot and correct the cause of the Major Internal Audit Failure alarm, refer to the "Major Internal Audit Failure - Audit (6)" section on page 2-17.

Minor Internal Audit Failure - Audit (7)

The Minor Internal Audit Failure alarm (minor) indicates that a minor internal audit failure has occurred. To troubleshoot and correct the cause of the Minor Internal Audit Failure alarm, refer to the "Minor Internal Audit Failure - Audit (7)" section on page 2-17.

Warning From Internal Audit - Audit (8)

The Warning From Internal Audit event serves as a warning that a problem with an internal audit has occurred. To correct the internal audit problem refer to the failure details (220), probable cause (80), and corrective actions (80) listed in the data field. Additionally, refer to the previous critical, major, and minor internal audit failure sections.

Softswitch Audit SIP CCB Release - Audit (9)

The Softswitch Audit SIP CCB Release event serves as a warning that one side of the BTS 10200 was inactive. To correct the primary cause of the event, let the SIA determine whether a network error or DNS error has occurred. The secondary cause of the event is that a software error has occurred. To correct the secondary cause of the event, contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Memory Audit Complete Status - Audit (10)

The Memory Audit Complete Status event serves as an informational alert that a SIP memory audit pass has been completed. The call data memory audit information should be checked to see if any call blocks have been cleared as a result of the audit. An investigation for root cause may be useful.

Critical Network Time Protocol Service Failure - Audit (11)

The Critical Network Time Protocol Service Failure alarm (critical) indicates that a critical Network Time Protocol (NTP) service failure has occurred. To troubleshoot and correct the cause of the Critical Network Time Protocol Service Failure alarm, refer to the "Critical Network Time Protocol Service Failure - Audit (11)" section on page 2-18.

Major Network Time Protocol Service Failure - Audit (12)

The Major Network Time Protocol Service Failure alarm (major) indicates that a major NTP service failure has occurred. To troubleshoot and correct the cause of the Major Network Time Protocol Service Failure alarm, refer to the "Major Network Time Protocol Service Failure - Audit (12)" section on page 2-18.

Minor Network Time Protocol Service Failure - Audit (13)

The Minor Network Time Protocol Service Failure alarm (minor) indicates that a minor NTP service failure has occurred. To troubleshoot and correct the cause of the Minor Network Time Protocol Service Failure alarm, refer to the "Minor Network Time Protocol Service Failure - Audit (13)" section on page 2-18.

Network Time Protocol Service Warning - Audit (14)

The Network Time Protocol Service Warning event serves as a warning that a problem with a NTP service has occurred. To correct the NTP service problem refer to the failure details (220), probable cause (80), and corrective actions (80) listed in the data field. Additionally, refer to the previous critical, major, and minor NTP service warning sections.

Critical Index Shared Memory Error - Audit (15)

The Critical Index Shared Memory Error alarm (critical) indicates that a critical shared memory index (IDX) error has occurred. To troubleshoot and correct the cause of the Critical Index Shared Memory Error alarm, refer to the "Critical Index Shared Memory Error - Audit (15)" section on page 2-18.

Process Heap Memory Usage Exceeds Minor Threshold Level - Audit (16)

The Process Heap Memory Usage Exceeds Minor Threshold Level alarm (minor) indicates that a process heap memory usage minor threshold level crossing has occurred. To troubleshoot and correct the cause of the Process Heap Memory Usage Exceeds Minor Threshold Level alarm, refer to the "Process Heap Memory Usage Exceeds Minor Threshold Level - Audit (16)" section on page 2-18.

Process Heap Memory Usage Exceeds Major Threshold Level - Audit (17)

The Process Heap Memory Usage Exceeds Major Threshold Level alarm (major) indicates that a process heap memory usage major threshold level crossing has occurred. To troubleshoot and correct the cause of the Process Heap Memory Usage Exceeds Major Threshold Level alarm, refer to the "Process Heap Memory Usage Exceeds Major Threshold Level - Audit (17)" section on page 2-18.

Process Heap Memory Usage Exceeds Critical Threshold Level - Audit (18)

The Process Heap Memory Usage Exceeds Critical Threshold Level alarm (critical) indicates that a process heap memory usage critical threshold level crossing has occurred. To troubleshoot and correct the cause of the Process Heap Memory Usage Exceeds Critical Threshold Level alarm, refer to the "Process Heap Memory Usage Exceeds Critical Threshold Level - Audit (18)" section on page 2-19.

Recovered Memory of Stale Call - Audit (19)

The Recovered Memory of Stale Call event serves as a warning that recovery of memory from a stale call has occurred. The primary cause of the warning is that a loss of communication with originating or terminating side occurred. To correct the primary cause of the warning, check if adjacent network element link is up and that the adjacent network element is properly communicating with the Cisco BTS 10200 Softswitch. The secondary cause of the warning is that an adjacent network device has a protocol error. To correct the secondary cause of the warning, check the adjacent network device protocol compatibility with the Cisco BTS 10200 Softswitch. The ternary cause of the warning is an internal software error. If a internal software error has occurred, contact Cisco to obtain technical assistance. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Audit Found Lost Call Data Record - Audit (20)

The Audit Found Lost Call Data Record alarm (major) indicates that an audit process has found a lost call data record. To troubleshoot and correct the cause of the Audit Found Lost Call Data Record alarm, refer to the "Audit Found Lost Call Data Record - Audit (20)" section on page 2-19.

Troubleshooting Audit Alarms

This section provides the information needed to troubleshoot and correct Audit alarms. Table 2-3 lists all Audit alarms in numerical order and provides cross reference to each subsection in this section.

Table 2-3 Cisco BTS 10200 Softswitch Audit Alarms

Alarm Type	Alarm Name	Alarm Severity
AUDIT(5)	Critical Internal Audit Failure - Audit (5)	CRITICAL
AUDIT(6)	Major Internal Audit Failure - Audit (6)	MAJOR
AUDIT(7)	Minor Internal Audit Failure - Audit (7)	MINOR
AUDIT(11)	Critical Network Time Protocol Service Failure - Audit (11)	CRITICAL
AUDIT(12)	Major Network Time Protocol Service Failure - Audit (12)	MAJOR
AUDIT(13)	Minor Network Time Protocol Service Failure - Audit (13)	MINOR
AUDIT(15)	Critical Index Shared Memory Error - Audit (15)	CRITICAL
AUDIT(16)	Process Heap Memory Usage Exceeds Minor Threshold Level - Audit (16)	MINOR
AUDIT(17)	Process Heap Memory Usage Exceeds Major Threshold Level - Audit (17)	MAJOR
AUDIT(18)	Process Heap Memory Usage Exceeds Critical Threshold Level - Audit (18)	CRITICAL
AUDIT(20)	Audit Found Lost Call Data Record - Audit (20)	MAJOR

Critical Internal Audit Failure - Audit (5)

The Critical Internal Audit Failure alarm (critical) indicates that a critical internal audit failure has occurred. To find the probable causes of the alarm, review the data field “Failure Details” and “Probable Causes” datawords. For the corrective actions for the alarm, review the data field “Corrective Actions” dataword. Once the “Corrective Actions” dataword has been reviewed, proceed with the corrective actions listed.

Major Internal Audit Failure - Audit (6)

The Major Internal Audit Failure alarm (major) indicates that a major internal audit failure has occurred. To find the probable causes of the alarm, review the data field “Failure Details” and “Probable Causes” datawords. For the corrective actions for the alarm, review the data field “Corrective Actions” dataword. Once the “Corrective Actions” dataword has been reviewed, proceed with the corrective actions listed.

Minor Internal Audit Failure - Audit (7)

The Minor Internal Audit Failure alarm (minor) indicates that a minor internal audit failure has occurred. To find the probable causes of the alarm, review the data field “Failure Details” and “Probable Causes” datawords. For the corrective actions for the alarm, review the data field “Corrective Actions” dataword. Once the “Corrective Actions” dataword has been reviewed, proceed with the corrective actions listed.

Critical Network Time Protocol Service Failure - Audit (11)

The Critical Network Time Protocol Service Failure alarm (critical) indicates that a critical NTP service failure has occurred. To find the probable causes of the alarm, review the data field “Failure Details” and “Probable Causes” datawords. For the corrective actions for the alarm, review the data field “Corrective Actions” dataword. Once the “Corrective Actions” dataword has been reviewed, proceed with the corrective actions listed.

Major Network Time Protocol Service Failure - Audit (12)

The Major Network Time Protocol Service Failure alarm (major) indicates that a major NTP service failure has occurred. To find the probable causes of the alarm, review the data field “Failure Details” and “Probable Causes” datawords. For the corrective actions for the alarm, review the data field “Corrective Actions” dataword. Once the “Corrective Actions” dataword has been reviewed, proceed with the corrective actions listed.

Minor Network Time Protocol Service Failure - Audit (13)

The Minor Network Time Protocol Service Failure alarm (minor) indicates that a minor NTP service failure has occurred. To find the probable causes of the alarm, review the data field “Failure Details” and “Probable Causes” datawords. For the corrective actions for the alarm, review the data field “Corrective Actions” dataword. Once the “Corrective Actions” dataword has been reviewed, proceed with the corrective actions listed.

Critical Index Shared Memory Error - Audit (15)

The Critical Index Shared Memory Error alarm (critical) indicates that a critical shared memory index error has occurred. To find the probable causes of the alarm, review the data field “Failure Details” and “Probable Causes” datawords. For the corrective actions for the alarm, review the data field “Corrective Actions” dataword. Once the “Corrective Actions” dataword has been reviewed, proceed with the corrective actions listed.

Process Heap Memory Usage Exceeds Minor Threshold Level - Audit (16)

The Process Heap Memory Usage Exceeds Minor Threshold Level alarm (minor) indicates that a process heap memory usage minor threshold level crossing has occurred. The primary cause of the alarm is that the increase in heap usage is due to a high call volume of traffic or a maintenance operation. Frequently monitor heap usage and see whether it is approaching major threshold level.

Process Heap Memory Usage Exceeds Major Threshold Level - Audit (17)

The Process Heap Memory Usage Exceeds Major Threshold Level alarm (major) indicates that a process heap memory usage major threshold level crossing has occurred. The primary cause of the alarm is that the increase in heap usage is due to a high call volume of traffic, a maintenance operation, a software problem. To isolate and correct the primary cause of the alarm, schedule a switchover during a maintenance window.

Process Heap Memory Usage Exceeds Critical Threshold Level - Audit (18)

The Process Heap Memory Usage Exceeds Critical Threshold Level alarm (critical) indicates that a process heap memory usage critical threshold level crossing has occurred. The primary cause of the alarm is that the increase in heap usage is due to a high call volume of traffic, a maintenance operation, a software problem. To isolate and correct the primary cause of the alarm, schedule a switchover during a maintenance window as soon as possible.

Audit Found Lost Call Data Record - Audit (20)

The Audit Found Lost Call Data Record alarm (major) indicates that an audit process has found a lost call data record. The primary cause of the alarm is that a software error has occurred; however, the orphaned records are recovered on detection 2d. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.