Carrier Voice over IP Fault Management Logs Reference (volume 3)

ATTENTION

Carrier Voice over IP Fault Management Logs Reference document uses six volumes to describe logs that Succession Portfolio components can generate. Not all components apply to every solution.

A log report is a message about an important conditions or events related to Succession portfolio component(s) performance. Log reports include, but are not restricted to, the following information:

- state and activity reports
- changes in state
- hardware or software errors
- test results
- other events or conditions that affect performance

Note: Both system actions and manual overrides can generate log reports.

Log formats

The log formats shown in this volume display in either NT or SCC2 standard formats. Not every format that generates from the core appears in a log report. Consult the latest software load that accompanies your product for a complete list of log formats.

In this volume

Volume 3 contains the following Succession logs by component:

- Policy Controller
- Session Server
- Universal Signaling Point

The tables in this volume identifies and briefly describes the logs they use. Double-click on the log identifier to see the log details.

Integrated Element Manager Server

The following table lists the individual logs that the Integrated Element Manager Server (IEMS) generates.

IEMS logs (Sheet 1 of 7)

Log ID	Description
BKM300	Indicates when a system backup fails
BKM600	Indicates when a system backup completes successfully
CSEM300	Indicates alarm sets and alarm clears for IEMS logs
CSEM600	Indicates INFO and unmapped logs for these logs
EMSS304	Indicates that the pam_mkhomedir module has timed out
EMSS315	Indicates the PAM login servlet health monitor detects the PAM login servlet is not functional
EMSS316	Indicates the pam_mkhomedir module cannot use the script that is owned by the user
EMSS317	Indicates the pam_mkhomedir module cannot get the script
EMSS318	Indicates the pam_mkhomedir module cannot continue since the euid is not root
EMSS319	Indicates the pam_is_authentication module cannot get the configuration file
EMSS325	Indicates the pam_is_authentication module cannot get the auth url
EMSS326	Indicates the pam_is_authentication module is blocked and timed out

IEMS logs (Sheet 2 of 7)

Log ID	Description
EMSS327	Indicates the script (default is mkhomedir) cannot access the directory or files
EMJS340	Indicates the state of communication between the Integrated EMS server and the device
EMJS341	Indicates that an SNMP data collection job fail
EMJS350	Indicates the state of the FTP connection with the device
EMJS360	Indicates the state of a report file
EMJS371	Indicates that no file is available to transfer
EMJS540	Indicates the status of a job
EMJS560	Indicates that the state of the Report Job
EMJS570	Indicates that the transfer job has resumed
EMJS640	Indicates that an SNMP OID mismatch has occurred
EMJS641	Indicates the successful completion of an SNMP data collection job
EMJS642	Indicates the partial completion of an SNMP data collection job
EMJS651	Indicates the successful completion of the CSV data collection job
EMJS652	Indicates the state of the CSV data collection job
EMJS661	Indicates the successful completion of a report job
EMJS662	Indicates the state of a report job
EMJS671	Indicates the completion of a transfer job
EMJS672	Indicates the failure of a transfer job
EMJS840	Indicates that an alarm threshold has reached the maximum value

IEMS logs (Sheet 3 of 7)

Log ID	Description
EMJS841	Indicates that the alarm threshold has returned to normal
EMSS300	Indicates that the client-side Pam + Radius SPI is unable to communicate with the server-side Radius interface
EMSS301	Indicates that there are problems with the server-side Radius proxy
EMSS302	Indicates that the IS PAM+ Plug-in fails to communicate with the Integrated EMS SPI
EMSS305	Indicates that the Identity Server (IS_ PAM+ Plug-in fails to communicate with the Integrated EMS SPI
EMSS306	Indicates that a packet from the Radius server is corrupted
EMSS307	Indicates that a packet from the Radius server has failed verification
EMSS308	Indicates that the client-side PAM+ Radius SPI is unable to communicate with the Radius Identity Server
EMSS309	Indicates that a packet from the Radius server does not contain all required fields
EMSS310	Indicates that the client configuration file cannot be opened
EMSS311	Indicates that the PAM+ Radius SPI is unable to communicate with the Radius Identity Server
EMSS312	Indicates that the client-side PAM+ Radius SPI is unable to update file systems
EMSS313	Indicates that the client-side PAM+ Radius SPI receives a accountExpiredException from the Radius server, regardless of the debug level set in the /etc/pam.conf file

IEMS logs (Sheet 4 of 7)

Log ID	Description
EMSS314	Indicates that the PAM+ Radius SPI receives a credentialExpiredException from the Radius server, regardless of the debug level set in the /etc/pam.conf file
EMSS320	Indicates there is a failure to initialize the single sign on (SSO) facility. SSO tokens will not be generated
EMSS321	Indicates there is a failure to authenticate the user due to an unhandled internal error
EMSS322	Indicates that no single-sign-on token is available after authentication
EMSS323	Indicates that no single-use tokens are generated due to an unhandled internal error
EMSS324	Indicates that the UNIX user's profile cannot be read due to an unhandled internal error
EMSS 600	Indicates that the PAM Radius daemon modifies the /etc/passwd or /etc/group files
EMSS 601	Indicates that there are successful or failed authentication requests of the authentication module
EMSS 602	Indicates successful or failed PAM SPI events from PAM + Plug-Ins
EMSS 603	Indicates a SunOne Identity Server Single Sign On (SSO) token activity for a token create event
EMSS 604	Indicates a SunOne Identity Server Single Sign On (SSO) token activity for a token destroy event
EMSS 605	Indicates a SunOne Identity Server Single Sign On (SSO) token activity for a token timeout event
IEMS398	Indicates Integrated EMS is unable to communicate with a managed device
IEMS399	Indicates that Integrated EMS regained communication with a managed device

IEMS logs (Sheet 5 of 7)

Log ID	Description
IEMS601	Indicates events raised from unknown devices
IEMS602	Indicates events raised from a known device
IEMS603	Indicates missed notifications
IEMS604	Indicates that a clear event is received from a device when there is no corresponding raise event in the Integrated EMS
IEMS605	Indicates when a manual alarm clear event is cleared manually
IEMS606	Indicates that the event count has exceeded the configured threshold limit or that the deletion of events is complete
IEMS607	Indicates there is a discrepancy in the active alarm list between Integrated EMS and the managed component
IEMS608	Indicates when the Integrated EMS Alarm Clearing Policy runs and detects alarms that exceed the configured maximum alarm age
IEMS609	Indicates when the Integrated EMS receives an event from one of its managed devices indicating the device or application has been restarte
IEMS610	Indicates when the Integrated EMS Diskspace Cleanup policy runs and detects the used space in the /data files system has exceeded the configured threshold in this policy
IEMS611	Indicates when the Integrated EMS Message Overload subsystem changes the state of a managed device from System Unmanaged or System Throttled back to Managed
IEMS612	Indicates when the Integrated EMS Message Overload subsystem detects a managed device that is pushing the Integrated EMS application server into an overload condition

IEMS logs (Sheet 6 of 7)

Log ID	Description
IEMS613	Indicates when the Integrated EMS Message Overload subsystem detects a managed device that is repeatedly pushing the Integrated EMS application server into an overload condition
NODE300	Indicates INM recovery actions when the node state is system busy
NODE323	Indicates when a REx request does not execute
NODE450	Summarize a series of event reports under one log header during a routine exercise (REX) test
SDM327	Indicates when a Network Time Protocol (NTP) problem is detected
SDM505	Indicates when the SuperNode Data Manager (SDM) high availability (SHA) process updates the SDM run state to offline
SDM627	Indicates when a Network Time Protocol (NTP) problem is cleared
SDM630	Indicate the SDM Routine EXercise (REX) start and stop time
SDMB360	Indicates when the connection to the Persistent Store System (PSS) is lost and cannot be restored
SDMB615	Indicates when a software-related error condition has been resolved
SDMB660	Indicates when a problem involving communications with other SuperNode Billing Application (SBA) features is resolved
SPM625	Generated when crossover message channels are not configured for SPMs
SPM710	Generated when the audit updates the ISDNPROT table
TMN301	Generated when an application error is detected
TMN302	Generated when a system error occurs.

IEMS logs (Sheet 7 of 7)

Log ID	Description
TMN303	Generated when a communication error occurs
TMN304	Generated when a connection error occurs
TMN309	Generated when a data server error occurs
TMN311	Generated when a fatal error occurs
TMN600	Generated by Log Normalizer when the normalizer process is successfully started and when delrep messages are sent successfully to the SDM OSF server
TMN601	Generated if the version summary file is not found, meaning that the archive is empty.
TMN604	Generated to provide information about application status
TMN605	Generated to provide Core restart information

Media Server 2000

The following table lists the individual logs that the Media Server 2000 generates.

Media Server 2000 logs (Sheet 1 of 2)

Log ID	Description
AMS300	Indicates a board reset on the Media Server 2000 node
AMS301	Indicates a fatal error the Media Server 2000 node
AMS302	Indicates a configuration error on the Media Server 2000 node
AMS303	Indicates a temperature alarm
AMS304	Indicates a feature key error on the Media Server 2000 node
AMS305	Indicates board call resource alarm on the Media Server 2000 node

Media Server 2000 logs (Sheet 2 of 2)

Log ID	Description
AMS306	Indicates a board controller failure alarm on the Media Server 2000 node
AMS307	Indicates an ethernet link alarm on the Media Server 2000 node
AMS308	Indicates a board overload on the Media Server 2000 node
AMS309	Indicates an active alarm table overflow on the Media Server 2000 node
AMS310	Indicates an ATM port alarm on the Media Server 2000 node
AMS311	Indicates an audio provisioning alarm on the Media Server 2000 node
AMS312	Indicates an operational state change on the Media Server 2000 node to “disabled”
AMS501	Indicates an admin state change on the Media Server 2000 node

Policy Controller

The following table lists the individual logs that the Policy Controller generates.

Policy Controller (Sheet 1 of 3)

Log ID	Description
SPCM300	Generated by the Policy Controller application maintenance process for a variety of informational purposes
SPCM301	Generated when the Policy Controller application, running on an enabled Policy Controller unit, is not in-service

Policy Controller (Sheet 2 of 3)

Log ID	Description
SPCM302	Generated when the Policy Controller application state goes out of sync between two Policy Controller units
SPCM500	Generated when the current state of the SIP application maintenance process changes from its last known state
SPCP301	Indicates that the Policy Controller application server signaling interface has a communication failure
SPCP302	Indicates that the Policy Controller has lost database connection
SPCP303	Indicates that the Application server request failure ratio exceeds the predefined threshold value
SPCP304	Indicates that the Policy Controller Endpoint Number exceeds the Endpoint Block Size
SPCP305	Indicates that the Policy Controller Endpoint Number exceeds the Endpoint Block Warning Size
SPCP501	Indicates that the Policy Controller application has started up
SPCP502	Indicates that the Policy Controller application has shut down
SPCP601	Indicates that a Flow Status Audit has completed
SPCP602	Indicates that a CAC request from the application server has been denied
SPCP603	Indicates that a the Policy Controller callp has accepted a topology change
SPCP604	Indicates that callP has detected that the Ingress Id of the Network Segment sent in a GateSet message from the GWC is not present in the Policy Controller database
TPM301	Indicates that the Topology Manager has lost database connection

Policy Controller (Sheet 3 of 3)

Log ID	Description
TPM501	Indicates that the Topology Manager application has started up
TPM502	Indicates that the Topology Manager application has shut down
TPM601	Indicates that the Topology Manager application has accepted a topology change

Session Server

The following table lists the individual logs that the Session Server generates.

Session Server logs (Sheet 1 of 6)

Log ID	Description
CRTM700	Generated when either option 1 (self-signed certificate) or option 2 (certificate signing request) is used during the execution of the Certificate Management Tool
CRTM701	Generated when option 1 (self-signed certificate) is used during the execution of the Certificate Management Tool
DBSE300	Generated any time a change in database connectivity is detected
SIPC301	Generated when the SIP Gateway Call Processing Application will not receive any incoming SIP messages
SIPC310	Indicates that “SIP CallP No Database Connection” is associated with the generation of the critical alarm due to a loss of connectivity
SIPC550	Generated when a Critical alarm is generated to a loss of connectivity between the database and the CallP application
SIPC650	Generated when the SIP Gateway Call Processing Application goes to get data from the database for a particular table and no data is found

Session Server logs (Sheet 2 of 6)

Log ID	Description
SIPC750	Generated when the SIP Gateway Call Processing Application drops incoming SIP messages due to Access Control List restrictions
SIPM300	Generated by the SIP Gateway application maintenance process for a variety of unexpected reasons or conditions
SIPM301	Generated when the SIPM301 critical alarm is raised
SIPM302	Generated when SIP Gateway application state goes out of sync between the two Session Server units
SIPM500	Generated with a SIP Maintenance State Change
SIPS300	Generated during the alarming of dropped connection requests.
SIPS301	Generated by authentication failure events
SIPS302	Generated as a result of regular alarm process checks to ensure the local server certificate continues to be valid
SIPS305	Generated during the initialization (unlock) of the SIP Gateway application
SIPS600	Generated during the connection setup of SIP Gateway application callp processes
SIPS601	Generated from TLS authentication failure events
SIPS604	Generated during initialization (unlock) of the SIP Gateway application, indicating when the current local certificate will expire
SIPS605	Generated during initialization (unlock) of the SIP Gateway application, indicating that TLS Security is enabled
SIPS606	Generated when there is a problem importing the trusted certificate provisioned into the database

Session Server logs (Sheet 3 of 6)

Log ID	Description
SIPS607	Indicates which remote server is not able to connect with the local server (SIP Gateway application running on the Session Server)
STGW700	Generated when callp activity is interrupted or negatively impacted
XTS300	Indicates that memory resources are low or near exhaustion
XTS301	Indicates that the CPU load average for one or more time segments has exceeded a preset threshold
XTS302	Indicates that free space on the root file system is low
XTS303	Indicates that at least one software process has terminated abnormally and may retain system resources such as memory space or CPU usage
XTS304	Indicates one or more of the Network File System (NFS) mounted file systems is inaccessible
XTS305	Indicates that the platform software lost time synchronization to one or more Network Time Protocol (NTP) servers, or the drift, is excessive
XTS306	Indicates that CPU utilization has exceeded a preset threshold
XTS309	Indicates that a peripheral hardware component has a PCI bus fault, Error Checking and Correction (ECC) memory fault, or a parity error
XTS314	Generated when application memory resources are running low
XTS315	Indicates that the standby call processing application on the inactive Session Server is not ready for takeover
XTS316	Indicates that the standby call processing application is out of service and the Session Server node is not operational

Session Server logs (Sheet 4 of 6)

Log ID	Description
XTS331	Indicates that the Session Server active unit cannot communicate to the mate unit through the ethernet connections
XTS335	Indicates that one of PTP ethernet interfaces is down
XTS336	Indicates that one or more ethernet links are unable to communicate with the network
XTS351	Indicates a response to several CON and APL alarms
XTS355	Indicates the inactive unit is jammed to prevent a Switch of Activity (SwAct)
XTS391	Indicates that a disk drive has certain major or minor alarms
XTS392	Indicates a error result has been returned from regularly occurring NGCL audit testing for any of a number of conditions
XTS395	Indicates a error result has been returned from regularly occurring NCGL file system audit tests
XTS600	Generated by the NCGL operating system when all the conditions which raised alarm XTS300 have been cleared
XTS601	Generated by the NCGL operating system when all the conditions which raised alarm XTS301 have been cleared
XTS602	Generated by the NCGL operating system when all the conditions which raised alarm XTS302 have been cleared
XTS603	Generated by the NCGL operating system when all the conditions which raised alarm XTS303 have been cleared
XTS604	Generated by the NCGL operating system when all the conditions which raised alarm XTS304 have been cleared

Session Server logs (Sheet 5 of 6)

Log ID	Description
XTS605	Generated by the NCGL operating system when all the conditions which raised alarm XTS305 have been cleared
XTS606	Generated by the NCGL operating system when all the conditions which raised alarm XTS306 have been cleared
XTS609	Generated by the NCGL operating system when all the conditions which raised alarm XTS309 have been cleared
XTS614	generated when all the conditions which raised alarm XTX314 are cleared
XTS615	Generated by the NCGL operating system when all the conditions which raised alarm XTS315 have been cleared
XTS616	Generated by the NCGL operating system when all the conditions which raised alarm XTS316 have been cleared
XTS631	Generated by the NCGL operating system when all the conditions which raised alarm XTS331 have been cleared
XTS635	Generated by the NCGL operating system when all the conditions which raised alarm XTS335 have been cleared
XTS636	Generated by the NCGL operating system when all the conditions which raised alarm XTS336 have been cleared
XTS651	Generated by the NCGL operating system when all the conditions which raised alarm XTS351 have been cleared
XTS655	Generated by the NCGL operating system when all the conditions which raised alarm XTS355 have been cleared
XTS670	Generated by the NCGL operating system when a SwAct of the system has been initiated

Session Server logs (Sheet 6 of 6)

Log ID	Description
XTS671	Generated by the NCGL operating system when a SwAct of the system has been completed
XTS691	Generated by the NCGL operating system when all the conditions which raised alarm XTS391 have been cleared
XTS692	Generated by the NCGL operating system when all the conditions which raised alarm XTS392 have been cleared
XTS695	Generated by the NCGL operating system when all the conditions which raised alarm XTS395 have been cleared

Universal Signaling Point

The following table lists the individual logs that the Universal Signaling Point (USP) generates.

Note: For more information about USP logs, refer to the *Log and Operational Measurement Descriptions for Universal Signaling Point (USP), version 3.0.3*. These logs also appear on the Graphical User Interface (GUI).

USP logs

Log ID	Description
USP398	Indicates an SNMP timeout in a USP device
USP399	Clears all other USP logs

Supplementary logs

The following documents reference logs and/or alarms that do not appear in this volume:

Note: The terms Passport, PVG and MDM have been re-branded in conjunction with the new Nortel Networks' brand simplified naming format. Passport is now referred to as the Nortel Networks Multiservice Switch, PVG is now the Nortel Networks Media Gateway 7480/15000, and MDM is now the Nortel Networks Multiservice Data

Manager.

- For XA-CORE logs, refer to the *XA-Core Reference Manual*, 297-8991-810.
- For information about Multiservice Switch alarms associated with your component, refer to *Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference*, NN10600-500 and *Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Overview PT-AAL1/UA-AAL1/UA-IP*, NN10092-911.

For information about Passport 8600 logs and traps, refer to the following documents:

- *Preside Passport 8600 Device Integration Cartridge User Guide*, 241-6003-110.
- *Configuring Network Management- Passport 8000 Series Software Release 3.5, 314723-B.*
- *System Messaging Platform Reference Guide- Passport 8000 Series Software Release 3.5, 315015-B.*

BKM300

The Synchronized Backup Manager (BKM) generates log report BKM300 when a system backup fails.

Format

The log report format for BKM300 is as follows:

```
Aug 23 21:00:01 BKM300 NONE INFO System Backup Failure
System backup failed. Reason: SESM not running.
```

Selected field descriptions

Descriptions for each field in the log report appear in the following table:

Field	Value	Description
Reason	Variable	Indicates the reason system backup failed

Action

Correct the problem in the system based on the failure reason. When the problem is corrected, re-attempt backup.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

BKM600

The Synchronized Backup Manager (BKM) generates log report BKM600 when a system backup completes successfully.

Format

The log report format for BKM600 is as follows:

```
Aug 23 21:00:01 BKM600 NONE INFO System Backup
Complete
System backup <yymmdd_hhmmss> completed successfully.
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CSEM300

Log report CSEM300 addresses a change of format for northbound events on the log feeds of Integrated EMS (IEMS) when used in conjunction with Core Element Manager (CEM).

Log report CSEM300 acts as an envelope to contain Communication Server 2000 (CS 2000) and SuperNode Data Manager (SDM) logs. The logs in the IEMS will be encapsulated inside log report CSEM300 in the northbound NT STD and SCC2 feeds. Log report CSEM300 indicates alarm sets and alarm clears for these logs. The northbound feeds from IEMS have new fields placed in them as indicated in the example in the Format section that follows.

The CEM is an optional component that allows the user to have an active alarm list in IEMS and SDM for CS 2000. The user can suppress logs (cause them to be removed) and un-suppress logs (cause them to be included) in the incoming log stream that the CEM receives from the Core. For information about suppressing and un-suppressing logs, refer to procedure "Specifying the logs delivered from the CM to the CS 2000 Core Manager" in *CS 2000 Core Manager Configuration Management*, NN10104-511.

Format

The log report format for CSEM300 is as follows:

Note: In the following format example, log SDM308 is encapsulated inside log CSEM300.

```
comp5iems  * CSEM300 FEB08 10:47:46 0515 TBL Alarm set
        Equip Id: 250Q SDM-0
        Notification Id: 0000007058
        Category: processingError
        Cause: backupFailure
        ComponentID: SDM-0
        LogKey: SDM308
        Description:
        "RTPU08AZ| |*  | |SDM308|FEB08|10:47:45|8441|
        TBL| SDM Base Maintenance
        System image backup (S-Tape) must be created
        Application Configuration Change.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
LogKey	variable	Indicates the original log name of the log encapsulated inside log CSEM300.

Action

This log report requires the action associated with the log identified in the LogKey field.

Associated OM registers

This log report has OM registers associated with the log identified in the LogKey field.

Additional information

This log report has the additional information associated with the log identified in the LogKey field.

CSEM600

Log report CSEM600 addresses a change of format for northbound events on the log feeds of Integrated EMS (IEMS) when used in conjunction with Core Element Manager (CEM).

Log report CSEM600 acts as an envelope to contain Communication Server 2000 (CS 2000) and SuperNode Data Manager (SDM) logs. The logs in the IEMS will be encapsulated inside log report CSEM600 in the northbound NT STD and SCC2 feeds. Log report CSEM600 indicates INFO and unmapped logs for these logs. The northbound feeds from IEMS have new fields placed in them as indicated in the example in the Format section that follows.

The CEM is an optional component that allows the user to have an active alarm list in IEMS and SDM for CS 2000. The user can suppress logs (cause them to be removed) and un-suppress logs (cause them to be included) in the incoming log stream that the CEM receives from the Core. For information about suppressing and un-suppressing logs, refer to procedure "Specifying the logs delivered from the CM to the CS 2000 Core Manager" in *CS 2000 Core Manager Configuration Management*, NN10104-511.

Format

The log report format for CSEM600 is as follows:

Note: In the following format example, log DDMS350 is encapsulated inside log CSEM600.

```
comp5iems    CSEM600 FEB08 10:48:32 0516 INFO Log
        Equip Id: 250Q SDM-0
        Notification Id: 0000007064
        Category: processingError
        Cause: ddmsINFO
        ComponentID: SDM-0
        LogKey: DDMS350
        Description:
       "RTPU08AZ| |***| |DDMS350|FEB08|10:48:30|8449|
        FAIL| Process Status
        Process Exception
        Subsystem: ddmsdcnh
        Terminated. Process shutdown.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
LogKey	variable	Indicates the original log name of the log encapsulated inside log CSEM600.

Action

This log report requires the action associated with the log identified in the LogKey field.

Associated OM registers

This log report has OM registers associated with the log identified in the LogKey field.

Additional information

This log report has the additional information associated with the log identified in the LogKey field.

EMJS340

Log report EMJS340 indicates the state of communication between the Integrated EMS server and the device.

The Integrated EMS generates log report EMJS340.

Format

The format for log report EMJS340 is as follows:

```
MSH10 * EMJS340 FEB25 11:45:19 7033 TBL IEMS OM Collec-
    tion Job Alarm
    Location: 10.102.15.138
    Job Instance: CollectionJob4
    State: Raise
    Category: processingError
    Cause: underlyingResourceUnavailable
    ComponentId:EMS-IEMS=10.102.15.138;Soft-
    ware=CollectionJob4;
    Time: Feb 25 11:45:19 2005
    Description:  Request  Timed  out  to  the  device
    0.0.0.0-PP8600
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the Integrated EMS server.
Job Instance	character string	Indicates the job name.
State	Raise, Clear	Indicates the state of the log.
ComponentId	character string	Indicates the details of the component.

Action

If the alarm condition persists, validate the state of the associated device. In addition, validate the associated configuration attributes in the IEMS and the associated device.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS341

Log report EMJS341indicates that an SNMP data collection job fails.

The Integrated EMS generates log report EMJS341.

Format

The format for log report EMJS341 is as follows:

```
MSH10 * EMJS341 FEB25 11:45:20 7034 TBL IEMS OM Collection Job Status
       Location: 10.102.15.138
       Job instance: CollectionJob4
       State: Raise
       Category: other
       Cause: communicationsSubsystemFailure
       ComponentID: EMS-IEMS=10.102.15.138,Software=CollectionJob4;
       Time: Feb 25 11:45:20 2005
       Description: Collection job CollectionJob4 unable to collect any
       attributes. Refer to the perf_log.txt debug log on the IEMS
       server
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	character string	Indicates the IP address of the Integrated EMS server.
Job Instance	character string	Indicates the job name.
Time	character string	Indicates the date and time of the log.
ComponentId	character string	Indicates the details of the component.

Action

If the alarm condition persists, analyze the perf_log.txt debug log on the Integrated EMS server.

Associated OM registers

This log report is associated with the following OMs:

- numOf60MinFailedCollectionJobs
- numOf24HrFailedCollectionJobs
- numOf12HrFailedCollectionJobs
- numOf5MinFailedCollectionJobs
- numOf15MinFailedCollectionJobs
- numOf30MinFailedCollectionJobs

Additional information

This log report requires no additional information.

EMJS350

Log report EMJS350 generated when the Integrated EMS encounters problems with an ftp session to a managed device, which is used to collect its associated OM data files.

The Integrated EMS generates log report EMJS350.

Format

The format for log report EMJS350 is as follows:

```
MSH10 **21 EMJS350 FEB25 14:27:13 1593 FLT IEMS OM Processing Job Alarm
       Location: msh10mdm0-MDM-Mgr-Unit-0
       Job instance: CollectionJob5,
       State: Raise
       Category: communications
       Cause: communicationsSubsystemFailure
       ComponentID: IEMS=10.102.15.138,Software=CollectionJob5;
       Time: Feb 25 14:27:13 2005
       Description: 5-min connection lost with the IP: 10.102.15.135
       Port:1650
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the Integrated EMS server.
Job Instance	character string	Indicates the job name.
ComponentId	character string	Indicates the details of the component.
Time	character string	Indicates the date and time of the log.
Description	character string	Indicates the state of the FTP connection with the device.

Action

If the alarm condition persists, validate the state of the associated device. In addition, validate the associated configuration attributes in the Integrated EMS and the associated device.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS360

Log report EMJS360 indicates the Integrated EMS has encountered a problem creating the CSV or XML output data file on the Integrated EMS server.

The Integrated EMS generates log report EMJS360.

Format

The formats for log report EMJS360 are as follows:

Example 1

The following example is for a raised alarm.

```
znc0s0jh     * EMJS360 MAY04 01:18:25 0060 TBL OM Report Job Alarm
            Location: 47.142.94.66
            Job instance: Test_sspfs_report
            State: Raise
            Category: processingError
            Cause: fileError
            ComponentId: EMS-IEMS=47.142.94.66;Software=Test_sspfs_report;
            SSPFS=znc0s0jh-SSPFS-Unit-0
            Time: May 04 01:18:25 2005
            Description: Error occurred while generating file.
            File Name: SSPFS.47.142.94.68-SSPFS.OMs.Test_sspfs_report.
            2005.05.04_01.18.25_EST.xml
```

Example 2

The following example is for a cleared alarm.

```
znc0s0jh      EMJS360 MAY04 01:30:13 0080 TBL OM Report Job Alarm
            Location: 47.142.94.66
            Job instance: Test_sspfs_report
            State: Clear
            Category: processingError
            Cause: fileError
            ComponentId: EMS-IEMS=47.142.94.66;Software=Test_sspfs_report;
            SSPFS=znc0s0jh-SSPFS-Unit-0
            Time: May 04 01:30:13 2005
            Description: Report file generation success.
            File Name: SSPFS.47.142.94.68-SSPFS.OMs.Test_sspfs_report.
            2005.05.04_01.30.13_EST.xml.gz
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the Integrated EMS server.
Job Instance	character string	Indicates the job name.
State	Raise, Clear	Indicates the state of the job report.
ComponentId	character string	Indicates the details of the component.
Time	character string	Indicates the date and time of the log.
FileName	character string	Indicates the file name that causes the error when the report file is generated.
Description	character string	Indicates the state of the report file generation.

Action

This log report implies that the IEMS OM collection subsystem is unable to successfully create the associated CSV or XML report file on the IEMS server. For detailed error information, monitor the perf_log.txt debug log on the IEMS server.

Associated OM registers

This log report has the associated OM: numOfFailedReportJobs.

Additional information

This log report requires no additional information.

EMJS371

Log report EMJS371 is generated when the Integrated EMS attempts to transfer the associated IEMS CSV or XML output file to a remote system but is unable to login to the remote system.

The Integrated EMS generates log report EMJS371.

Format

The format for log report EMJS371 is as follows:

```
MSH10 * EMJS371 FEB25 13:59:59 1430 TBL IEMS OM Processing Job Alarm
      Location: 10.102.15.138
      Job instance: TransferJob7
      State: Raise
      Category: communications
      Cause: transmitFailure
      ComponentID: EMS-IEMS=10.102.15.138,Software=TransferJob7;
      Time: Feb 25 13:59:59 2005
      Description: Login incorrect.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the Integrated EMS server.
Job Instance	character string	Indicates the job name.
ComponentId	character string	Indicates the details of the component.
Time	character string	Indicates the date and time of the log.
File name	character string	Indicates the filename.
Destination	IP address	Indicates the IP address of the destination.

Action

Verify the associated IEMS transfer job is configured with a valid userid and password.

Associated OM registers

This log report has the following associated OMs:

- numOf12HrFailedTransferJobs
- numOf24HrFailedTransferJobs
- numOf5MinFailedTransferJobs
- numOf60MinFailedTransferJobs
- numOf30MinFailedTransferJobs
- numOf15MinFailedTransferJobs

Additional information

This log report requires no additional information.

EMJS540

Log report EMJS540 is generated when the state of an Integrated EMS collection job has been changed.

The Integrated EMS generates log report EMJS540.

Format

The format for log report EMJS540 is as follows:

```
MSH10    EMJS540 FEB25 14:41:59 1681 <OFFL/RTS> OM Collection Job
         Status
         Location: 10.102.15.138
         Job Instance: CollectionJob12
         State: <Resumed/Enabled/Disabled/Suspended>
         Category: other
         ComponentID:EMS-IEMS=10.102.15.138,Software=CollectionJob12
         Time: Feb 25 14:41:59 2005
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the Integrated EMS server.
Job Instance	character string	Indicates the job name.
State	Resumed, Enabled, Disabled, Suspended	Indicates the state of the job.
ComponentId	character string	Indicates the details of the component.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS560

Log report EMJS560 indicates the state of an Integrated EMS report job has been changed.

The Integrated EMS generates log report EMJS560.

Format

The format for log report EMJS560 is as follows:

```
MSH10   EMJS560 FEB25 14:43:15 1690 <OFFL/RTS> OM Report Job Status
       Location: 10.102.15.138
       Job Instance: ReportJob13
       State: <Suspended/Resumed/Disabled/Enabled>
       Category: other
       ComponentID: EMS-IEMS=10.102.15.138,Software=ReportJob13
       Time: Feb 25 14:43:15 2005
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Job Instance	character string	Indicates the job name.
State	Suspended, Resumed, Disabled, Enabled	Indicates the state of the job.
Component Id	character string	Indicates the IP address and job name of the device.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS570

Log report EMJS570 indicates the state of an Integrated EMS transfer job has been changed.

The Integrated EMS generates log report EMJS570.

Format

The format for log report EMJS570 is as follows:

```
MSH10   EMJS570 FEB25 14:43:15 1690 <OFFL/RTS> OM Transfer Job Status
       Location: 10.102.15.138
       Job Instance: ReportJob13
       State: <Suspended/Resumed/Disabled/Enabled>
       Category: other
       ComponentID: EMS-IEMS=10.102.15.138,Software=ReportJob13
       Time: Feb 25 14:43:15 2005
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the Integrated EMS server.
Job Instance	character string	Indicates the job name.
State	Suspended, Resumed, Disabled, Enabled	Indicates the state of the job.
Component Id	character string	Indicates the details of the component.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS640

Log report EMJS640 is generated by the IEMS OM collection sub-system when errors are detected when parsing the collected CSV input file or attempting to collect data from an SNMP device. When parsing a collected CSV file, the event description will indicate the associated line number in the file that cannot be parsed. When attempting to collect data from an SNMP-based device, the event description will list the OIDs that could not be collected.

Format

The format for log report EMJS640 is as follows:

```
MSH10   EMJS640 FEB25 14:00:18 1432 INFO IEMS OM Collection Job Status
      Location: 10.102.15.138
      Job instance: CollectionJob4
      State: Info
      Category: processingError
      Cause: datasetProblem
      ComponentID:EMS-IEMS=10.102.15.138;Software+CollectionJob4;
      Invalid OID List: .1.3.6.1.4.2272.1.100.9.11.1.5, .1.3.6.1.4.1.
      2272.1.100.9.11.1.4
      Time: Feb 25 14:00:18 2005
      Description: SNMP OID data collection failure for
      192.168.2.57-PP8600
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the Integrated EMS server.
Job Instance	character string	Indicates the job name.
ComponentId	character string	Indicates the details of the component.
Time	character string	Indicates the date and time of the log.

Action

For detailed error information, monitor the perf_log.txt debug log on the Integrated EMS server.

Associated OM registers

This log report has the following associated OMs:

- numOf15MinParitalSuccessfulJobs
- numOf12HrParitalSuccessfulJobs
- numOf24HrParitalSuccessfulJobs
- numOf30MinParitalSuccessfulJobs
- numOf5MinParitalSuccessfulJobs
- numOf60MinParitalSuccessfulJobs

Additional information

This log report requires no additional information.

EMJS641

Log report EMJS641 indicates the successful completion of an SNMP data collection job.

The Integrated EMS generates log report EMJS641.

Format

The format for log report EMJS641 is as follows:

```
MSH10    EMJS641 FEB25 14:10:36 1482 INFO IEMS OM Collection Job
       Status
       Location: 10.102.15.138
       Job Instance: CollectionJob4
       State: Successful
       Category: other
       ComponentID: EMS-IEMS=10.102.15.138,Software=CollectionJob4;
       Time: Feb 25 14:10:36 2005
       Description: Processing successfully done for the MOs:
       [10.102.15.130-PP8600, 10.102.15.131-PP8600,
       192.168.2.54-PP8600, 192.168.2.57-PP8600]
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the Integrated EMS server.
Job Instance	character string	Indicates the job name.
ComponentId	character string	Indicates the details of the component.

Action

This log report requires no action.

Associated OM registers

This log report has the following associated OMs:

- numOf24HrSuccessfulJobs
- numOf60MinSuccessfulJobs
- numOf12HrSuccessfulJobs
- numOf30MinSuccessfulJobs
- numOf5MinSuccessfulJobs
- numOf15MinSuccessfulJobs

Additional information

This log report requires no additional information.

EMJS642

Log report EMJS642 is generated when the Integrated EMS is unable to collect the OM data for all the devices configured in an IEMS collection job.

The Integrated EMS generates log report EMJS642.

Format

The format for log report EMJS642 is as follows:

```
MSH10   EMJS642 FEB25 18:55:27 3711 INFO IEMS OM Collection Job Status
      Location: 10.102.15.138
      Job instance: CollectionJob11
      State: Incomplete
      Category: other
      ComponentID: EMS-IEMS=10.102.15.138,Software=CollectionJob11;
      Time: Feb 25 18:55:27 2005
      Description: Collection job CollectionJob11 unable to collect
      all attributes. Refer to the perf_log.txt debug log file on the
      IEMS server
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the Integrated EMS server.
Job Instance	character string	Indicates the job name.
ComponentId	character string	Indicates the details of the component.

Action

For detailed error information, monitor the perf_log.txt debug log file on the Integrated EMS server.

Associated OM registers

This log report has the following associated OMs:

- numOf15MinPartialSuccessfulJobs
- numOf12HrPartialSuccessfulJobs
- numOf24HrPartialSuccessfulJobs

- numOf30MinPartialSuccessfulJobs
- numOf5MinPartialSuccessfulJobs
- numOf60MinPartialSuccessfulJobs

Additional information

This log report requires no additional information.

EMJS651

Log report EMJS651 indicates the successful completion of the CSV data collection job.

The Integrated EMS generates log report EMJS651.

Format

The format for log report EMJS651 is as follows:

```
MSH10    EMJS651 FEB25 14:26:13 1587 INFO IEMS OM Processing Job Status
         Location: 10.102.15.138
         Job Instance: CollectionJob12
         State: Successful
         Category: other
         ComponentID: EMS-IEMS=10.102.15.138,Software=CollectionJob12;
         Time: Feb 25 14:26:13 2005
         Description: Processing successfully done for the MOs:
         [IEMS-Mgr]
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the Integrated EMS server.
Job Instance	character string	Indicates the job name.
ComponentID	character string	Indicates the details of the component.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS652

Log report EMJS652 is generated to report the failure of a CSV or MDM collection job.

The Integrated EMS generates log report EMJS652.

Format

The format for log report EMJS652 is as follows:

```
MSH10   EMJS652 MAR04 17:30:15 0495 INFO IEMS OM Processing Job Status
      Location: 47.142.94.68
      Job Instance: mscColl_AM
      State: Failure
      Category: other
      ComponentID: EMS-IEMS=47.142.94.68,Software=mcsColl_AM;
      Time: Mar 04 17:30:15 2005
      Description: Invalid file format
      File Name: {wnc0y0ns.us.nortel.com-CSE-Mgr=No files available in
      the Directory (/export/home/maint/omDir/mcsOMfiles/SM_0/AM1_0/csv)
      to process. Check done for the MO :
      wnc0y0ns.us.nortel.com-CSE-Mgr}
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the Integrated EMS server.
Job Instance	character string	Indicates the job name.
State	Incomplete, Failure	Indicates the state of the job.
ComponentId	character string	Indicates the details of the component.

Action

For detailed error information, monitor the perf_log.txt debug log on the Integrated EMS server.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS661

Log report EMJS661 indicates the successful completion of a report job.

The Integrated EMS generates log report EMJS661.

Format

The format for log report EMJS661 is as follows:

```
MSH10    EMJS661 FEB25 14:26:23 1589 INFO IEMS OM Report Job Status
       Location: 10.102.15.138
       Job instance: ReportJob6
       State: Successful
       Category: other
       ComponentID: EMS-IEMS=10.102.15.138,Software=ReportJob6;
       Time: Feb 25 14:26:23 2005
       Description: /data/oms/1
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the Integrated EMS server.
Job Instance	character string	Indicates the job name.
Component Id	character string	Indicates the details of the component.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS662

Log report EMJS662 is generated to report the failure of an Integrated EMS report job.

The Integrated EMS generates log report EMJS662.

Format

The format for log report EMJS662 is as follows:

```
znc0s0jh   EMJS662 MAY02 04:25:00 0142 TBL IEMS OM Report Job Status
     Location: 47.142.94.66
     Job Instance: iems_report
     State: Failure
     Category: processingError
     Cause: fileError
     ComponentID: EMS-IEMS=47.142.94.66,Software=iems_report;
     Time: May 02 04:25:00 2005
     Description: /data/oms/1
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the Integrated EMS server.
Job Instance	character string	Indicates the job name.
State	Incomplete, Failure	Indicates the state of the job - Incomplete or Failure.
Time	character string	Indicates the date and time of the log.
ComponentId	character string	Indicates the details of the component.
Equipment identifier	IP address	Indicates the hostname on which the Integrated EMS server is running

Action

For detailed error information, monitor the perf_log.txt debug log on the Integrated EMS server.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS671

Log report EMJS671 indicates the status of a transfer job.

The Integrated EMS generates log report EMJS671.

Format

The format for log report EMJS671 is as follows:

```
MSH10  EMJS671 MAR31 00:40:06 3811 INFO IEMS OM Transfer Job Status
      Location: 10.102.15.138
      Job instance: TransferJob14
      State: Successful
      Category: other
      ComponentID: EMS-IEMS=10.102.15.138,Software=TransferJob14;
      Time: Mar 31:00:40:06 2005
      Description: TransferJob14 job has been executed successfully
      FileName :  GWC.10.102.15.48-GWC.OMs.GWCREPORT2005.03.31_00.40.02_
      EST.xml.gz
      Destination: 10.102.15.18
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the Integrated EMS server.
Job Instance	character string	Indicates the job name.
ComponentID	character string	Indicates the details of the component.
Destination	IP address	Indicates the name of the device to which the file is transferred.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS672

Log report EMJS672 indicates the failure of a transfer job.

The Integrated EMS generates log report EMJS672.

Format

The format for log report EMJS672 is as follows:

```
znc0s0jh    EMJS672 MAY02 09:11:32 0502 TBL IEMS OM Transfer Job Status
        Location: 47.142.94.66
        Job instance: sspfs_tran
        State: Incomplete
        Category: other
        ComponentID: EMS-IEMS=47.142.94.66,Software=sspfs_tran;
        Time: May 02 09:11:32 2005
        File Name:
        SSPFS.47.142.94.68-SSPFS.OMs.bob.2005.05.02_07.38.14_EST.csv.
        gz,
        Destination: 47.142.94.68
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the Integrated EMS server.
Job Instance	character string	Indicates the job name.
State	Incomplete	Indicates the state of the job.
Time	character string	Indicates the date and time of the log.
ComponentId	character string	Indicates the details of the component.
FileName	character string	Indicates the file name.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS840

Log report EMJS840 is generated when the Integrated EMS OM collection subsystem detects that a collected attribute has exceeded a configured threshold.

The Integrated EMS generates log report EMJS840.

Format

The format for log report EMJS840 is as follows:

```
znc0s0jh *** EMJS840 MAY04 00:48:35 0008 TBL Threshold Alarm
      Location: 47.142.94.66
      Job Instance: sspfs
      Time: May 04 00:48:35 2005
      State: Critical
      Category: Threshold
      Cause: Threshold Alarm
      ComponentID: EMS-IEMS=47.142.94.66;Software=sspfs;Node=47.142.94.68
      Monitored Value: iplnReceives
      Collected Value: 13271720
      Threshold Type: max
      Threshold: 100
      Rearm Value: 80
      Description: Threshold Exceeded
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Job Instance	character string	Indicates the job name.
Time	character string	Indicates the date and time of the log.
Component Id	character string	Indicates the IP address, job name and node ID of the device.
Monitored Value	character string	Indicates the OID for which the data is collected.

Field	Value	Description
Collected Value	integer	Indicates the actual value collected from the device for this OID.
Threshold type	character string	Indicates the threshold type based on the configured threshold (Max/Min/Equal).
Threshold	integer	Indicates the actual threshold value configured for a threshold.
Rearm Value	integer	Indicates the actual rearm value configured for a threshold.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS841

Log report EMJS841is generated when the Integrated EMS OM collection subsystem detects that a collected attribute dropped below a configured threshold value. This log is used to clear the alarm event raised in the log report EMJS840 event.

The Integrated EMS generates log report EMJS841.

Format

The format for log report EMJS841 is as follows:

```
znc0s0jh   EMJS841 MAY04 00:52:15 0020 TBL Threshold Alarm
       Location: 47.142.94.66
       Job Instance: sspfs
       Time: May 04 00:52:15 2005
       State: Clear
       Category: Threshold
       Cause: Threshold Alarm
       ComponentID: EMS-IEMS=47.142.94.66;Software=sspfs;Node=
       47.142.94.68
       Monitored Value: iplnReceives
       Collected Value: 13273301
       Threshold type: max
       Description: Collected Value is below the Threshold limit.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Job Instance	character string	Indicates the job name.
Time	character string	Indicates the date and time of the log.
Component Id	character string	Indicates the IP address, job name and node ID of the device.
Monitored Value	character string	Indicates the OID for which the data is collected.

Field	Value	Description
Collected Value	integer	Indicates the actual value collected from the device for this OID.
Threshold type	character string	Indicates the threshold type based on the configured threshold (Max/Min/Equal).

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS300

Log report EMSS300 indicates that the client-side PAM + Radius SPI is unable to communicate with the server-side Radius interface.

Note: This log is sent directly to syslog through the standard UNIX syslog C API.

The Integrated EMS generates log report EMSS300.

Format

The format for log report EMS300 is as follows:

```
znc0s0jh    EMSS300 JUN30 11:09:16 0721 INFO EMSS^M
          Location: <CLIENT - hostname>
          Time: Jun 30 11:09:16
          Category: communicationsAlarm
          Probable Cause: connectionEstablishmentError
          Component Id: PAM+ Radius SPI
          Description: RADIUS server <SERVER-hostname> failed to
          respond.
          Recovery Action: Please verify network connectivity for both
          client and server machines; verify the RADIUS server is
          running.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	communications Alarm	Indicates the category of the alarm.
Probable cause	connection Establishment Error	Indicates the probable cause of the alarm.
Client-hostname	character string	Indicates the hostname of the client.
Time	character string	Indicates the date and time of the log.
Server-hostname	character string	Indicates the hostname of the server.

Action

Verify network connectivity for both client and server machines. Verify that the Radius server is running.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS301

Log report EMSS301 indicates that a problem is detected by the Radius server in the process of handling a given authentication request. These problems are unexpected exceptions detected by Radius server plugins. These problems can be due to incorrect Radius server setup or the unavailability of a critical Radius server dependency.

The Integrated EMS generates log report EMSS301.

Format

The format for log report EMS301 is as follows:

```
znc0s0jh    EMSS301 JUN30 11:09:16 0721 INFO EMSS^M
           <Device name:device port> EMSS
           Location: <SERVER - hostname>
           Time: Jun 30 11:09:16
           Category: processingErrorAlarm
           Probable Cause: outOfService
           Component Id: Radius Proxy
           Description: <LoginException message from Radius>
           Recovery Action: Check the status of the Sun IS and restart if
           necessary.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	outOfService	Indicates the probable cause of the alarm.
Device name:device port	character string	Indicates the device name and device port.
Time	character string	Indicates the date and time of the log.
SERVER - hostname	character string	Indicates the server and hostname.

Action

Check the status of the SunOne Identity Server (S1 IS) and restart if necessary.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS302

Log report EMSS302 indicates that the Radius policy plugin detects no single-sign-on token. This indicates that there is a problem with the Sun Identity Server or that the Sun Identity Server is not running.

The Integrated EMS generates log report EMSS302.

Format

The format for log report EMSS302 is as follows:

```
znc0s0jh    EMSS302 JUN30 11:09:16 0721 INFO EMSS^M
           <Device name:device port> EMSS
           Location: <SERVER - hostname>
           Time: Jun 30 11:09:16
           Category: processingErrorAlarm
           Probable Cause: outOfService
           Component Id: Radius Proxy
           Description: No single-sign-on token available
           after authentication.
           Recovery Action: Check the status of Sun IS and restart if
           necessary.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm
Probable Cause	outOfService	Indicates the probable cause of the alarm
Device name:device port	character string	Indicates the device name and device port.
application name	character string	Indicates the application name.
Time	character string	Indicates the date and time of the log.
SERVER - hostname	character string	Indicates the server and hostname.

Action

Check the status of the Sun Identity Server and restart if necessary.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS304

Log report EMSS304 indicates that the pam_mkhomedir module has timed out. This log is produced when the pam_mkhomedir module invokes the script mkhomedir, but the script does not return within the timeout period (default 30 seconds).

The Integrated EMS generates log report EMSS304.

Format

The format for log report EMSS304 is as follows:

```
znc0s0jh    EMSS304 JUN30 11:09:16 0721 INFO EMSS^M
          Location: <CLIENT - hostname>
          Time: Jun 30 11:09:16
          Category: processingErrorAlarm
          Probable Cause: timeoutExpired
          Component Id: PAM MAKE HOME DIRECTORY SPI
          Description: Authentication with a pthread was timed out
          (30 seconds)
          Recovery Action: The process running the script file (script_
          name) might not work properly and blocked the main process
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	timeoutExpired	Indicates the probable cause of the alarm.
Client-hostname	character string	Indicates the hostname of the client.
Time	character string	Indicates the date and time of the log.
Server-hostname	character string	Indicates the hostname of the server.

Action

Check the process running the script and kill it if necessary.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS305

Log report EMSS305 indicates that the client side PAM+ Radius SPI is unable to communicate with the server-side Radius interface.

The Integrated EMS generates log report EMSS305.

Format

The format for log report EMSS305 is as follows:

```
znc0s0jh    EMSS305 JUN30 11:09:16 0721 INFO EMSS^M
          Location: <SERVER - hostname>
          Time: Jun 30 11:09:16
          Category: communicationsAlarm
          Probable Cause: communicationsProtocolError
          Component Id: PAM+ Radius SPI
          Description: Error reading packet from RADIUS server <SERVER -
          hostname>
          Recovery Action: Please verify network connectivity for both
          client and server machines; verify server is running.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	communications Alarm	Indicates the category of the alarm.
Probable cause	communications ProtocolError	Indicates the probable cause of the alarm.
Time	character string	Indicates the date and time of the log.
SERVER - hostname	character string	Indicates the server and hostname.

Action

Verify network connectivity for both client and server machines. Verify that the Radius server is running.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS306

Log report EMSS306 indicates that a packet from the Radius server is corrupted. The PAM+ Radius SPI is unable to communicate with the Radius Identity Server.

Note: Log report EMSS306 is sent directly to syslog through the standard Unix syslog C API.

The Integrated EMS generates log report EMSS306.

Format

The format for log report EMSS306 is as follows:

```
znc0s0jh    EMSS306 JUN30 11:09:16 0721 INFO EMSS^M
   Location: <SERVER - hostname>
   Time: Jun 30 11:09:16
   Category: communicationsAlarm
   Probable Cause: communicationsProtocolError
   Component Id: PAM+ Radius SPI
   Description: RADIUS packet from server <SERVER - hostname>
   is corrupted.
   Recovery Action: Please verify network connectivity for both client
   and server machines; verify RADIUS server is running.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	communications Alarm	Indicates the category of the alarm.
Probable cause	communications ProtocolError	Indicates the probable cause of the alarm.
Time	character string	Indicates the date and time of the log.
SERVER - hostname	character string	Indicates the server and hostname.

Action

Verify network connectivity for both client and server machines. Verify that the server is running.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS307

Log report EMSS307 indicates that a packet from the Radius server has failed verification. The PAM+ Radius SPI is unable to communicate with the Radius Identity Server.

Note: Log report EMSS307 is sent directly to syslog through the standard Unix syslog C API.

The Integrated EMS generates log report EMSS307.

Format

The format for log report EMSS307 is as follows:

```
znc0s0jh    EMSS307 JUN30 11:09:16 0721 INFO EMSS^M
   Location: <SERVER - hostname>
   Time: Jun 30 11:09:16
   Category: communicationsAlarm
   Probable Cause: communicationsProtocolError
   Component Id: PAM+ Radius SPI
   Description: Packet from RADIUS server <SERVER - hostname>
   fails verification.
   Recovery Action: Please verify network connectivity for both client
   and server machines; verify RADIUS server is running and that the
   shared secret is correct.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	communications Alarm	Indicates the category of the alarm.
Probable cause	communications ProtocolError	Indicates the probable cause of the alarm.
Time	character string	Indicates the date and time of the log.
SERVER - hostname	character string	Indicates the server and hostname.

Action

Verify network connectivity for both client and server machines. Verify that the server is running and that the shared secret is correct.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS308

Log report EMSS308 indicates that the client-side PAM+ Radius SPI is unable to communicate with the Radius Identity Server.

Note: Log report EMSS308 is sent directly to syslog through the standard Unix syslog C API.

The Integrated EMS generates log report EMSS308.

Format

The format for log report EMSS308 is as follows:

```
znc0s0jh    EMSS308 JUN30 11:09:16 0721 INFO EMSS^M
   Location: <SERVER - hostname>
   Time: Jun 30 11:09:16
   Category: communicationsAlarm
   Probable Cause: invalidMessageReceived
   Component Id: PAM+ Radius SPI
   Description: Response packet from RADIUS server <SERVER - hostname>
   does not match the request packet id.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	communications Alarm	Indicates the category of the alarm.
Probable cause	invalidMessage Received	Indicates the probable cause of the alarm.
Time	character string	Indicates the date and time of the log.
SERVER - hostname	character string	Indicates the server and hostname.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS309

Log report EMSS309 indicates that a packet from the Radius server does not contain all required fields. The client-side PAM+ Radius SPI is unable to communicate with the Radius Identity Server.

Note: Log report EMSS309 is sent directly to syslog through the standard Unix syslog C API.

The Integrated EMS generates log report EMSS309.

Format

The format for log report EMSS309 is as follows:

```
znc0s0jh    EMSS309 JUN30 11:09:16 0721 INFO EMSS^M
   Location: <SERVER - hostname>
   Time: Jun 30 11:09:16
   Category: communicationsAlarm
   Probable Cause: invalidMessageReceived
   Component Id: PAM+ Radius SPI
   Description: Packet from RADIUS server <SERVER - hostname>
   does not contain all required fields.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	communications Alarm	Indicates the category of the alarm.
Probable cause	invalidMessage Received	Indicates the probable cause of the alarm.
Time	character string	Indicates the date and time of the log.
SERVER - hostname	character string	Indicates the server and hostname.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS310

Log report EMSS310 indicates that the client configuration file cannot be opened. The PAM+ Radius SPI is unable to communicate with the Radius Identity Server.

Note: Log report EMSS310 is sent directly to syslog through the standard Unix syslog C API.

The Integrated EMS generates log report EMSS310.

Format

The format for log report EMSS310 is as follows:

```
znc0s0jh    EMSS310 JUN30 11:09:16 0721 INFO EMSS^M
   Location: <SERVER - hostname>
   Time: Jun 30 11:09:16
   Category: processingErrorAlarm
   Probable Cause: fileError
   Component Id: PAM+ Radius SPI
   Description: Could not open client configuration file.
   Recovery Action: Please verify access to /etc/raddb/server on the
   client machine.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.
Time	character string	Indicates the date and time of the log.
SERVER - hostname	character string	Indicates the server and hostname.

Action

Verify network connectivity for both client and server machines. Verify that the server is running and that the configuration file is accessible.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS311

Log report EMSS311 indicates that the PAM+ Radius SPI is unable to communicate with the Radius Identity Server.

Note: Log report EMSS311 is sent directly to syslog through the standard Unix syslog C API.

The Integrated EMS generates log report EMSS311.

Format

The format for log report EMSS311 is as follows:

```
znc0s0jh    EMSS311 JUN30 11:09:16 0721 INFO EMSS^M
   Location: <SERVER - hostname>
   Time: Jun 30 11:09:16
   Category: processingErrorAlarm
   Probable Cause: fileError
   Component Id: PAM+ Radius SPI
   Description: Failed to read hostname or secret.
   Recovery Action: Please verify access to /etc/raddb/server on the
   client machine.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.
Time	character string	Indicates the date and time of the log.
SERVER - hostname	character string	Indicates the server and hostname.

Action

Verify network connectivity for both client and server machines. Verify that the server is running and that /etc/raddb/server is available on the client machine.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS312

Log report EMSS312 indicates that the pam_mkhomedir module is not able to retrieve user information from the NSSwitch. This log is produced when the pam_mkhomedir module attempts to retrieve user information from the NSSwitch by using getpwnam and fails.

Note: Log report EMSS312 is sent directly to syslog through the standard Unix syslog C API.

The Integrated EMS generates log report EMSS312.

Format

The format for log report EMSS312 is as follows:

```
znc0s0jh    EMSS312 JUN30 11:09:16 0721 INFO EMSS^M
   Location: <SERVER - hostname>
   Time: Jun 30 11:09:16
   Category: processingErrorAlarm
   Probable Cause: fileError
   Component Id: PAM MAKE HOME DIRECTORY SPI
   Description: Not able to do getpwnam with the user: (user_name) due
   the error: (error message).
   Recovery Action: Check NSSwitch configuration and ensure it works
   with the user
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.
Time	character string	Indicates the date and time of the log.
SERVER - hostname	character string	Indicates the server and hostname.

Action

Check the NSSwitch configuration and ensure it works with the user.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS313

Log report EMSS313 indicates the radius server monitor detects the radius process is not functional.

Note: This log report is sent directly to syslog through the "logger" Unix utility.

Format

The format for log report EMSS313 is as follows:

```
znc0s0jh    EMSS313 JUN30 11:09:16 0721 INFO EMSS^M
          Location: 47.142.94.68
          Time: Jun 30 11:09:16
          Category: processingErrorAlarm
          Probable Cause: outOfService
          Component Id: CLASS=SYS;SYSTYPE=SECMon;SECMonComp=RADSVR
          Description: RADSVR is unhealthy, will restart if currently
          running.^M
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	outOfService	Indicates the probable cause of the alarm.

Action

The health monitor automatically attempts to restart the radius server if the radius server is running.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS314

Log report EMSS314 indicates the identity server health monitor detects the server process is not functional.

Note: This log report is sent directly to syslog through the "logger" Unix utility.

Format

The format for this log report is as follows:

```
znc0s0jh    EMSS314 JUN30 11:09:16 0721 INFO EMSS^M
          Location: 47.142.94.68
          Time: Jun 30 11:09:16
          Category: processingErrorAlarm
          Probable Cause: outOfService
          Component Id: CLASS=SYS;SYSTYPE=SECMon;SECMonComp=IS
          Description: Identity Server (IS) is unhealthy, will restart
          if currently running.^M
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	outOfService	Indicates the probable cause of the alarm.

Action

The health monitor automatically attempts to restart the identity server if the identity server is running.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS315

Log report EMSS315 indicates the PAM login servlet health monitor detects the PAM login servlet is not functional.

The Integrated EMS generates log report EMSS315.

Format

The format for log report EMSS315 is as follows:

```
znc0s0jh    EMSS315 JUN30 11:09:16 0721 INFO EMSS^M
          Location: <CLIENT - hostname>
          Time: Jun 30 11:09:16
          Category: processingErrorAlarm
          Probable Cause: outOfService
          Component Id: CLASS=SYS;SYSTYPE=SECMon;SECMonComp=WEBSERVICES
          Description: PAM login servlet is unhealthy, restarting
          WEBSERVICES.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	outOfService	Indicates the probable cause of the alarm.

Action

The health monitor automatically attempts to restart WEBSERVICES through servman if it is running already.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS316

Log report EMSS316 indicates the pam_mkhomedir module cannot use the script that is owned by the user.

The Integrated EMS generates log report EMSS316.

Format

The format for log report EMSS316 is as follows:

```
znc0s0jh    EMSS316 JUN30 11:09:16 0721 INFO EMSS^M
          Location: <CLIENT - hostname>
          Time: Jun 30 11:09:16
          Category: processingErrorAlarm
          Probable Cause: fileError
          Component Id: PAM MAKE HOME DIRECTORY SPI
          Description: Not able to use the script (script_name) since
          the ownership of the script is not root
          Recovery Action: Change the ownership of the script file to
          root
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.

Action

Check the ownership of the script and change the owner to root.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS317

Log report EMSS317 indicates the pam_mkhomedir module cannot get the script.

The Integrated EMS generates log report EMSS317.

Format

The format for log report EMSS317 is as follows:

```
znc0s0jh    EMSS317 JUN30 11:09:16 0721 INFO EMSS^M
          Location: <CLIENT - hostname>
          Time: Jun 30 11:09:16
          Category: processingErrorAlarm
          Probable Cause: fileError
          Component Id: PAM MAKE HOME DIRECTORY SPI
          Description: Not able to use the script (script_name) due to
          (file errors)
          Recovery Action: Please verify if the script file (script_
          name) exists
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.

Action

Verify the script is available and the name of the script is correct.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS318

Log report EMSS318 indicates the pam_mkhomedir module cannot continue since the euid is not root.

The Integrated EMS generates log report EMSS318.

Format

The format for log report EMSS318 is as follows:

```
znc0s0jh    EMSS318 JUN30 11:09:16 0721 INFO EMSS^M
          Location: <CLIENT - hostname>
          Time: Jun 30 11:09:16
          Category: processingErrorAlarm
          Probable Cause: fileError
          Component Id: PAM MAKE HOME DIRECTORY SPI
          Description: No permissions to continue since the euid of the
          current process is not root: (uid)
          Recovery Action: The effective user id of the process has to
          be root
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.

Action

Make sure the effective user id of the process running the module is root.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS319

Log report EMSS319 indicates the pam_is_authentication module cannot get the configuration file.

The Integrated EMS generates log report EMSS319.

Format

The format for log report EMSS319 is as follows:

```
znc0s0jh    EMSS319 JUN30 11:09:16 0721 INFO EMSS^M
          Location: <CLIENT - hostname>
          Time: Jun 30 11:09:16
          Category: processingErrorAlarm
          Probable Cause: fileError
          Component Id: PAM IS AUTHENTICATION SPI
          Description: Could not get IS auth configuration file: (file_
          name)
          Recovery Action: Please provide an IS auth config file with
          pam opetion conf=/dir/file, or put you is auth config file
          in the default location
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.

Action

Verify if the configuration file is on the location configured by the pam option of if it is on the default location.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS320

Log report EMSS320 indicates the pam_is_authentication module cannot read the configuration file. This log is produced when the module attempts to read the contents of the configuration file but fails.

The Integrated EMS generates log report EMSS320.

Format

The format for log report EMSS320 is as follows:

```
znc0s0jh    EMSS320 JUN30 11:09:16 0721 INFO EMSS^M
          Location: <SERVER - hostname>
          Time: Jun 30 11:09:16
          Category: processingErrorAlarm
          Probable Cause: fileError
          Component Id: PAM IS AUTHENTICATION SPI
          Description: Could not open the IS auth configuration file
          (file_name)
          Recovery Action: Please verify the permissions of file
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.
Server-hostname	character string	Indicates the hostname of the server.
Location	character string	Indicates the server and hostname.
Time	character string	Indicates the date and time of the log.

Action

Configure and start the SunOne Identity Server (S1 IS). Then restart the Tomcat servlet engine.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS321

Log report EMSS321 indicates the pam_is_authentication module cannot get the auth url.

The Integrated EMS generates log report EMSS321.

Format

The format for log report EMSS321 is as follows:

```
znc0s0jh    EMSS321 JUN30 11:09:16 0721 INFO EMSS^M
          Location: <SERVER - hostname>
          Time: Jun 30 11:09:16
          Category: processingErrorAlarm
          Probable Cause: fileError
          Component Id: PAM IS AUTHENTICATION SPI
          Description: Missing IS auth url from the config file (file_
          name)
          Recovery Action: Please verify the auth url is set correctly
          in the config file: (file_name)
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.
Location	character string	Indicates the server and hostname.
Time	character string	Indicates the date and time of the log.

Action

Verify the auth url option is set correctly from the configuration file.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS322

Log report EMSS322 indicates the pam_is_authentication module is blocked and timed out.

The Integrated EMS generates log report EMSS322.

Format

The format for log report EMSS322 is as follows:

```
znc0s0jh    EMSS322 JUN30 11:09:16 0721 INFO EMSS^M
          Location: <SERVER - hostname>
          Time: Jun 30 11:09:16
          Category: processingErrorAlarm
          Probable Cause: timeoutExpired
          Component Id: PAM IS AUTHENTICATION SPI
          Description: Authentication was blocked and timed out
          (seconds of timeout)
          Recovery Action: Please check if IS processes work properly
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	timeoutExpired	Indicates the probable cause of the alarm.
Location	character string	Indicates the server and hostname.
Time	character string	Indicates the date and time of the log.

Action

Verify the IS processes work properly. Restart IS processes if necessary.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS323

Log report EMSS323 indicates the pam_is_authentication module cannot get the configuration file.

The Integrated EMS generates log report EMSS323.

Format

The format for log report EMSS323 is as follows:

```
znc0s0jh    EMSS323 JUN30 11:09:16 0721 INFO EMSS^M
          Location: <SERVER - hostname>
          Time: Jun 30 11:09:16
          Category: processingErrorAlarm
          Probable Cause: fileError
          Component Id: PAM IS VALIDATION SPI
          Description: Could not get IS auth configuration file:
          (file_name)
          Recovery Action: Please provide an IS auth config file with
          pam opetion conf=/dir/file, or put you is auth config file in
          the default location
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm
Probable cause	fileError	Indicates the probable cause of the alarm.
Location	character string	Indicates the server and hostname.
Time	character string	Indicates the date and time of the log.

Action

Verify if the configuration file is on the location configured by the pam option or if it is on the default location.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS324

Log report EMSS324 indicates the pam_is_module cannot read the configuration file.

The Integrated EMS generates log report EMSS324.

Format

The format for log report EMSS324 is as follows:

```
znc0s0jh    EMSS324 JUN30 11:09:16 0721 INFO EMSS^M
          Location: <SERVER - hostname>
          Time: Jun 30 11:09:16
          Category: processingErrorAlarm
          Probable Cause: fileError
          Component Id: PAM IS VALIDATION SPI
          Description: Could not open the IS auth configuration file
          (file_name)
          Recovery Action: Please verify the permissions of file
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.
Location	character string	Indicates the server and hostname.
Time	character string	Indicates the date and time of the log.

Action

Verify the configuration file is readable.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS325

Log report EMSS325 indicates the pam_is_authentication module cannot get the auth url.

The Integrated EMS generates log report EMSS325.

Format

The format for log report EMSS325 is as follows:

```
znc0s0jh    EMSS325 JUN30 11:09:16 0721 INFO EMSS^M
          Location: <CLIENT - hostname>
          Time: Jun 30 11:09:16
          Category: processingErrorAlarm
          Probable Cause: fileError
          Component Id: PAM IS VALIDATION SPI
          Description: Missing IS auth url from the config file (file_
          name)
          Recovery Action: Please verify the auth url is set correctly
          in the config file: (file_name)
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.

Action

Verify the auth url option is set correctly from the configuration file.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS326

Log report EMSS326 indicates the pam_is_authentication module is blocked and timed out.

The Integrated EMS generates log report EMSS326.

Format

The format for log report EMSS326 is as follows:

```
znc0s0jh    EMSS326 JUN30 11:09:16 0721 INFO EMSS^M
          Location: <CLIENT - hostname>
          Time: Jun 30 11:09:16
          Category: processingErrorAlarm
          Probable Cause: timeoutExpired
          Component Id: PAM IS VALIDATION SPI
          Description: Validation was blocked and timed out (seconds of
          timeout)
          Recovery Action: Please check if IS processes work properly
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	timeoutExpired	Indicates the probable cause of the alarm.

Action

Verify the IS processes work properly. Restart the IS processes if necessary.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS327

Log report EMSS327 indicates the script (default is mkhomedir) cannot access the directory or files.

The Integrated EMS generates log report EMSS327.

Format

The format for log report EMSS327 is as follows:

```
znc0s0jh    EMSS327 JUN30 11:09:16 0721 INFO EMSS^M
          Location: <CLIENT - hostname>
          Time: Jun 30 11:09:16
          Category: processingErrorAlarm
          Probable Cause: fileError
          Component Id: PAM Make Home Directory SPI
          Description: File/Directory access error when executing the
          script (script_name)
          Recovery Action: Please perform actions according to the
          error message: (error message)
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.

Action

Verify the directory files are available and accessible. The error messages show which files or directories to check.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS 600

Log report EMSS 600 indicates that the PAM Radius daemon modifies the /etc/passwd or /etc/group files.

The Integrated EMS generates log report EMSS 600.

Format

The format for log report EMS 600 is as follows:

```
EMSS600 mmmdd hh:mm:ss NONE INFO <Device name:device port>
<application name>
Message: System files have been updated
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Device name:device port	character string	Indicates the device name and device port.
application name	character string	Indicates the application name.

Action

This log report is for information only.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS 601

Log report EMSS 601 indicates that there are successful or failed authentication requests of the authentication module.

The Integrated EMS generates log report EMSS 601.

Format

The format for log report EMS 601 is as follows:

```
EMSS601 mmmdd hh:mm:ss NONE INFO <Device name:device port>
<application name>
Message: <Successful (Failed) authentication attempt>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Device name:device port	character string	Indicates the device name and device port.
application name	character string	Indicates the application name.
Successful (Failed authentication attempt	character string	Indicates whether the authentication request is successful or has failed.

Action

This log report is for information only.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS 602

Log report EMSS 602 indicates successful or failed PAM SPI events from PAM + Plug-Ins.

The Integrated EMS generates log report EMSS 602.

Format

The format for log report EMS 602 is as follows:

```
EMSS602 mmmdd hh:mm:ss NONE INFO <Device name:device port>
<application name>
Message: Authentication successful/failed
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Device name:device port	character string	Indicates the device name and device port.
application name	character string	Indicates the application name.

Action

This log report is for information only.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS 603

Log report EMSS 603 indicates a SunOne Identity Server Single Sign On (SSO) token activity for a token create event. Sensitive token information is not included in these logs.

The Integrated EMS generates log report EMSS 603.

Format

The format for log report EMS 603 is as follows:

```
mmm dd hh:mm:ss <Device name:device port> Thread-28:
SESSION CREATE: uid=administrator, ou=People,
o=ca.nortel.com
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Device name:device port	character string	Indicates the device name and device port.

Action

This log report is for information only.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS 604

Log report EMSS 604 indicates a SunOne Identity Server Single Sign On (SSO) token activity for a token destroy event. Sensitive token information is not included in these logs.

The Integrated EMS generates log report EMSS 604.

Format

The format for log report EMS 604 is as follows:

```
mmm dd hh:mm:ss <device name:device port>Thread-28
DESTROY: uid=administrator, ou=People, o=ca.nortel.com"
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
device name:device port	character string	Indicates the device name and device port.

Action

This log report is for information only.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS 605

Log report EMSS 605 indicates a SunOne Identity Server Single Sign On (SSO) token activity for a token timeout event. Sensitive token information is not included in these logs.

The Integrated EMS generates log report EMSS 605.

Format

The format for log report EMS 605 is as follows:

```
mmm dd hh:mm:ss <device name:device port> Thread-28:
IDLE TIMEOUT:uid=amAdmin, ou=People, o=ca.nortel.com"
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
device name:device port	character string	Indicates the device name and device port.

Action

This log report is for information only.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEMS398

Log report IEMS398 indicates Integrated EMS is unable to communicate with a managed device.

The Integrated EMS generates log report IEMS398.

Format

The format for log report IEMS398 is as follows:

```
CABLAB *** IEMS398 DEC03 17:46:59 5150 FLT Communication Lost
        Location: 47.135.43.7
        Motification ID: 0
        State: Raised
        Category: Communications
        Cause: Communications subsystem failure
        Time: Dec 03 17:46:59 2004
        ComponentId: ucary118c.ca.nortel.com
        Specific Problem: Connection Lost
        Description: IEMS Unable to communicate with managed device
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the IEMS server.
Time	character string	Indicates the date and time of the log.
Component Id	character string	Indicates the name of the device.

Action

This log report requires the user to check network connectivity and device status to identify the cause of the communication failure.

Associated OM registers

This log report has the following associated OMs:

- numOfUnKnownDeviceStateTransitions
- numOfDevicesInUnKnownState

Additional information

This log report requires no additional information.

IEMS399

Log report IEMS399 indicates that Integrated EMS regained communication with a managed device.

The Integrated EMS generates log report IEMS399.

Format

The format for log report IEMS399 is as follows:

```
CABLAB    IEMS399 DEC03 17:47:49 5164 FLT Communication Regained
        Location: 47.135.43.7
        Notification ID: 0
        State: Cleared
        Category: Communications
        Time: Dec 03 17:47:49 2004
        Component Id: ucary118c.ca.nortel.com
        Description: IEMS regained communication with the managed device
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the IEMS server.
Time	character string	Indicates the date and time of the log.
Component Id	character string	Indicates the name of the device.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEMS601

Log report IEMS601 is generated when the IEMS receives an event from a device that is not configured in the IEMS inventory.

The Integrated EMS generates log report IEMS601.

Format

The format for log report IEMS601 is as follows:

```
MSH10    IEMS601 MAR31 00:39.45 3805 INFO
       Location: 10.102.29.6
       Event: .1.3.6.1.6.3.1.1.5.1
       Varbind0: .1.3.6.1.2.1.1.3.0: 0 hours, 0 minutes, 0 seconds.
       Varbind1: .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.1
```

Selected field descriptions

This log report has no selected field descriptions.

Action

This log report requires no action.

Associated OM registers

This log report has the following associated OMs:

- numOfEventsFromUnknownDevices
- numOfEventsFromUnknownSNMPDevices
- numOfEventsFromUnknownCustlogDevices

Additional information

This log report requires no additional information.

IEMS602

Log report IEMS602 is generated when the Integrated EMS receives an event from a device in the IEMS inventory but the event type is not recognized.

The Integrated EMS generates log report IEMS602.

Format

The format for log report IEMS602 is as follows:

```
MSH10     IEMS602 MAR31 00:39:37 3799 INFO Fault
         Location: 10.102.15.152
         Event: .1.3.6.1.6.3.1.1.5.4
         Varbind0: .1.3.6.1.2.1.1.3.0: 0 hours, 0 minutes, 16 seconds.
         Varbind1: .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.4
         Varbind2: .1.3.6.1.2.1.2.2.1.1.1: 1
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the device that sent the associated event.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEMS603

Log report IEMS603 is generated when the Integrated EMS detects a gap in the sequence numbers for the events it is receiving from one of its managed devices.

The Integrated EMS generates log report IEMS603.

Format

The format for log report IEMS603 is as follows:

```
MSH10    IEMS603 MAR31 12:01:29 9939 INFO Missed Notifications
        Location: 10.102.15.138
        Component Id: IEMS=msh10ptm-SAM21-Mgr
        Time: Mar 31 12:01:29 2005
        Description: Notification(s) missed in ML 112 - 237
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IEMS IP address.
Component name	character string	Indicates the component name of the device.
Time	character string	Indicates the date and time of the log.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEMS604

Log report IEMS604 indicates that a clear event is received from a device when there is no corresponding raise event in the Integrated EMS.

The Integrated EMS generates log report IEMS604.

Format

The format for log report IEMS604 is as follows:

```
MSH10      IEMS604 FEB25 22:44:35 1118 INFO Cleared
         Location: Storm_san;47.166.56.10
         Notification Id: 201
         State: Cleared
         Time: Feb 25 22:44:35 2005
         ComponentId: STORMIA=langley40
         Description: Status: Alarm cleared. One minute load average is
         0.00. Five minute load average is 0.01. Fifteen minute load aver-
         age is 0.06.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	character string;IP address	Indicates the display name and IP address of the managed device.
Time	character string	Indicates the date and time of the log.
Component Id	character string	Indicates the component name.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEMS605

Log report IEMS605 is generated when a manual alarm clear event is cleared manually.

The Integrated EMS generates log report IEMS605.

Format

The format for log report IEMS605 is as follows:

```
CABLAB    IEMS605 MAR31 00:01:15 3162
        Location: 10.102.15.138
        Description: Manually cleared by iemsadm
        Correlation ID: 825548401
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the IEMS server.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEMS606

Log report IEMS606 indicates that the event count has exceeded the configured threshold limit or that the deletion of events is complete.

The Integrated EMS generates log report IEMS606.

Format

The format for log report IEMS606 is as follows:

```
RTPO    IEMS606 MAR01 11:12:36 5928 INFO Database Fault
       Location: IEMS-Mgr (47.142.110.40)
       State: INFO
       Time: Mar 01 11:13:59 2005
       Maximum No.of Event 1000000
       Event count: 2116289
       Description: Deletion of Events completed. The total number of
       events deleted:1216289
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the log.
Maximum No. of Event	character string	Indicates the maximum number of events allowed before an event is generated.
Event count	character string	Indicates the total number of events in the database prior to the cleanup policy running.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEMS607

Log report IEMS607 indicates there is a discrepancy in the active alarm list between Integrated EMS and the managed component. The discrepancy is found through alarm resynchronization. Differing alarm lists can occur when alarms have cleared in the managed component, but the clear log has not reached Integrated EMS. In order to keep the downstream OSSs up to date, Integrated EMS creates log report IEMS607.

The Integrated EMS generates log report IEMS607.

Format

The format for log report IEMS607 is as follows:

```
MSH10   IEMS607 MAR31 00:40:13 3826 INFO IEMS Autogenerated Clear
       Location: CICM-000-B;10.102.15.153
       NotificationID: 14
       State: Clear
       Time: Mar 31 00:40:13 2005
       Specific Problem: Mate node failed - Broadcast failure and ask
       components to promote to Master.
       Category: equipment
       Component Id: CICM=CICM-000-B;NodeType=Cicm
       Description: Raised log: CICM334; Audit: Mate Node Failed
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	character string;IP address	Indicates the display name and IP address of the managed device.
NotificationID	Integer	Indicates the notification Id field value from the database.
Time	character string	Indicates the date and time of the log.
Category	character string	Indicates the alarm category of the log.
Component Id	character string	Indicates the component Id field.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEMS608

Log report IEMS608 is generated when the Integrated EMS Alarm Clearing Policy runs and detects alarms that exceed the configured maximum alarm age. This policy is run for the device types that have been included in this policy.

The Integrated EMS generates log report IEMS608.

Format

The format for log report IEMS608 is as follows:

```
RTPO    IEMS608 MAR01 14:31:27 4881 INFO IEMS Alarm Aged Clear
       Location: 8600 (Calvin);47.142.110.252
       NotificationID:
       State: Clear
       Time: Mar 01 14:31:27 2005
       Specific Problem: Generic Link Status
       Category: communications
       Component Id: PP8600=47.142.110.252; ifIndex=467
       Description: Raised log: PP317; Link Down: ifIndex = 467( Admin-
       Status = up OperationStatus = down)
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	character string;IP address	Indicates the display name and IP address of the managed device.
NotificationID	Integer	Indicates the notification Id field value from the database.
Time	character string	Indicates the date and time of the log.
Category	character string	Indicates the alarm category of the log.
Component Id	character string	Indicates the component Id field.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEMS609

Log report IEMS609 is generated when the Integrated EMS receives an event from one of its managed devices indicating the device or application has been restarted. This indicates the entire active alarm list for this device has been cleared.

The Integrated EMS generates log report IEMS609.

Format

The format for log report IEMS609 is as follows:

```
znc0s0jh    IEMS609 MAR06 08:42:57 5053 INFO IEMS Alarm List Cleared
          Location: 47.142.94.68;47.142.94.68
          NotificationID: 0
          State: Clear
          Time: Mar 06 08:42:57 2005
          Specific Problem: IEMS cleared its active alarm list for the man-
          aged component.
          Category: other
          Component Id: NE-STORM=Storm_san;47.166.56.10
          Description: IEMS has received some kind of cold start or reset
          message from the managed component and has cleared its active
          alarm list for it. Any alarm issues still present in the managed
          component after its startup will be re-raised again.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IEMS display name and IP address.
NotificationID	Integer	Indicates the notification Id field value from the database.
Time	character string	Indicates the date and time of the log.
Category	character string	Indicates the alarm category of the log.
Component Id	character string	Indicates the component Id field.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEMS610

Log report IEMS610 is generated when the Integrated EMS Diskspace Cleanup policy runs and detects the used space in the /data files system has exceeded the configured threshold in this policy. When this policy runs, it removes the oldest stored OM directories in the /data/Oms directory that contain the IEMS output OM CSV or XML data files. This cleanup policy attempts to reduce the used space in the /data file system below the configured threshold in this policy. If this policy is unable to reduce the used space below the configured threshold, this event will be generated.

The Integrated EMS generates log report IEMS610.

Format

The format for log report IEMS610 is as follows:

```
znc0s0jh    IEMS610 MAR08 13:49:26 0011 INFO Diskspace Fault
          Location: IEMS-Mgr; 47.142.94.68
          ComponentID: IEMS-Mgr
          Time: Mar 08 13:49:26 2005
          Description: /data disk partition space exceeds 80%. The dir's
          deleted under /data/oms/ are:. Only ./1 is left. No further
          action taken. Partition still exceeds threshold!!
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Component Id	character string	Indicates the component Id field.

Action

If log report IEMS609 is generated, evaluate and clean up the files in the /data file system.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEMS611

Log report IEMS611 is generated when the Integrated EMS Message Overload subsystem changes the state of a managed device from System Unmanaged or System Throttled back to Managed. This event is used to clear the alarm states raised by the IEMS612 and IEMS613 events.

The Integrated EMS generates log report IEMS611.

Format

The format for log report IEMS611 is as follows:

```
znc0s0jh    IEMS611 APR16 09:18:41 0829 INFO Fault Interface Normal
          Location: 47.142.128.86
          Time: Apr 16 09:18:41 2005
          ComponentId: comp5iems-CEM-Mgr
          Description: Managed as IEMS System is back to normal
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the Integrated EMS.
Component Id	character string	Indicates the component Id field.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEMS612

Log report IEMS612 is generated when the Integrated EMS Message Overload subsystem detects a managed device that is pushing the Integrated EMS application server into an overload condition. The state of the device is changed from Managed to System Throttled to attempt to recover from the message overload condition.

The Integrated EMS generates log report IEMS612.

Format

The format for log report IEMS612 is as follows:

```
CABLAB *  IEMS612 APR16 09:18:39 0828 TBL Fault Interface Overloaded
        Location: 47.142.128.86
        State: Raised
        Time: Apr 16 09:18:39 2005
        ComponentId: comp5iems-CEM-Mgr
        Specific Problem: Message Overload
        Description: Throttle Unmanaged as IEMS System is overloaded
        with too many Messages
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the IEMS server.
Time	character string	Indicates the date and time of the log.
Component Id	character string	Indicates the name of the device.

Action

Investigate why this device is sending excessive message rates.

Associated OM registers

This log report has the following associated OMs:

- numOfDevicesInThrottledState
- numOfThrottledDeviceStateTransitions

Additional information

This log report requires no additional information.

IEMS613

Log report IEMS613 is generated when the Integrated EMS Message Overload subsystem detects a managed device that is repeatedly pushing the Integrated EMS application server into an overload condition. The state of the device is changed from Managed to System Unmanaged to attempt to recover from the message overload condition.

The Integrated EMS generates log report IEMS613.

Format

The format for log report IEMS613 is as follows:

```
CABLAB *  IEMS613 APR16 09:18:39 0828 TBL Fault Interface Overloaded
        Location: 47.142.128.86
        State: Raised
        Time: Apr 16 09:18:39 2005
        ComponentId: comp5iems-CEM-Mgr
        Specific Problem: Message Overload
        Description: Throttle Unmanaged as IEMS System is overloaded
        with too many Messages
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the IEMS server.
Time	character string	Indicates the date and time of the log.
Component Id	character string	Indicates the name of the device.

Action

Investigate why this device is sending excessive message rates.

Associated OM registers

This log report has the following associated OMs:

- numOfDevicesInSystemUnManagedState
- numOfSystemUnManagedDeviceStateTransitions

Additional information

This log report requires no additional information.

NODE300

Integrated Node Maintenance (INM) generates log report NODE300 when a trouble condition is present with the node. This report indicates INM recovery actions when the node state is system busy.

The resource maintenance manager (RMM) reports faults to the INM when the system executes the QueryPM faults command at the MAP display.

Format

The log report format for NODE300 is as follows:

```
NODE300 mmmdd hh:mm:ss ssdd INFO TBL Warning
  Location=<node>
  Status=<trouble_status>
  Trouble=<trouble_code>
  Action=<user_action>
  Integrated Node Maintenance Detailed Information
  Trouble Reason=<INM trouble condition reason>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
trouble_code	variable	Identifies the reason for the problem.
user_action	variable	Identifies the action to take.
INM trouble condition reason	variable	Provides a reason for the trouble condition.

Action

Check the trouble field. Take action as indicated in the user action field.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

NODE323

Integrated Node Maintenance (INM) generates log report NODE323 when a REx request does not execute.

Format

The log report format for NODE323 is as follows:

```
NODE323 mmmdd hh:mm:ss ssdd TBL REx Fault
  Location: <location>
  Status: <alarm_status>
  Trouble: <trouble>
  Action: <action>
  REX did not run
  Units: <units_not_RExed>
  Reason: <reason>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
location	character string	Indicates the location of the PM to which the event applies.
alarm_status	alarm raised	Indicates an alarmed log. ***Note:*** An alarmed log means that double stars at the beginning of the format highlight the log report. An alarmed log does not mean a MAP alarm is present.
trouble	character string	Identifies the reason for the problem.
action	character string	Indicates the trouble log is for information only.
units_not_RExed	0, 1, 0 and 1	Indicates the units that did not run the REx.
reason	character string	Indicates the reason the REx did not run.

Action

Clear the reason that did not allow the REx to run. This reason can require a manual maintenance action or a waiting period for a system operation to clear a trouble condition. Contact the next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

NODE450

Integrated Node Maintenance (INM) generates log report NODE450 to summarize a series of event reports under one log header during a routine exercise (REX) test. The NODE450 log is never in alarm mode. This log is an abbreviated summary of the routine series of operations that compose a REX test.

The system reports all trouble events (faults) as separate logs to make them more accessible to mechanized downstream analysis. High priority events are logged as the events reach the central log system. Other events are logged following the generation of NODE450. Events of the INITIATE class appear only in NODE450, and never as separate logs.

Format

The log report formats for NODE450 are as follows:

Format 1

```
NODE450 mmmdd hh:mm:ss ssdd SUMM REX TEST SUMMARY
  Location: <entity name>
  Summary: REX Test Sequence Successful
```

Format 2

```
NODE450 mmmdd hh:mm:ss ssdd SUMM REX TEST SUMMARY
  Location: <entity name>
  Summary: REX Test Sequence Failed
  TIME            EVENT
  <hh:mm:ss>      <detailed event type>
  <hh:mm:ss>      <detailed event type>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	Symbolic text	Indicates the name of the hardware or software component or service involved.
Summary	REX Test Sequence Successful or REX Test Sequence Failed	Indicates success or failure of the REX test.
TIME	Integers	If REX test failed, indicates the time (hh:mm:ss).
EVENT	Symbolic text	If REX test failed, indicates the event.

Action

The NODE 450 log report helps log analysis by bringing together related events in one report, in the correct time sequence. The action required, if any, depends on the nature of the repeated events.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM327

The subsystem generates log SDM327 when a Network Time Protocol (NTP) problem is detected.

Format

The log report format for SDM327 is as follows:

```
RTP_com4iems ** SDM327 SEP18 11:22:15 1724 TBL SDM
        Base Maintenance
        NTP problem detected
        Reason: NTP is not synchronized.
```

Selected field descriptions

This log report has no selected field descriptions.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM505

The subsystem generates log SDM505 when the SuperNode Data Manager (SDM) high availability (SHA) process updates the SDM run state to offline. The system sends this log to the operations support system (OSS). The user cannot view this report at the SDM remote maintenance menu. The log that the custlog file stores has a slightly different format than the following one.

Format

The log report format for SDM505 is as follows:

```
SDM505 mmmdd hh:mm:ss ssdd OFFL SDM Base Maintenance
SMD state change to OFFL
From: <old_state>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
old_state	MANB	Indicates the previous state of the SDM is MANB.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM627

The subsystem generates log SDM627 when a Network Time Protocol (NTP) problem is cleared.

Format

The SDM format for log report SDM627 is as follows:

```
RTP_com4iems    SDM627 SEP17 20:09:15 5984 INFO SDM
        Base Maintenance
        NTP problem cleared
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM630

The subsystem generates log SDM630 to indicate the SDM Routine EXercise (REX) start and stop time.

Format

The log report formats for SDM630 are as follows:

REX started

```
RTP_com4iems    SDM630 SEP18 11:22:15 1724 NONE INFO
SDM REX started
```

REX complete

```
RTP_com4iems    SDM630 SEP18 11:22:15 1724 NONE INFO
SDM REX complete
```

Selected field descriptions

This log report has no selected field descriptions.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDMB360

The SuperNode Data Manager Billing (SDMB) subsystem generates log SDMB360 when it loses and cannot restore the connection to the Persistent Store System (PSS). This log is associated with the alarm SDM Billing Application Interface (SBAIF).

Format

The log report format for SDMB360 is as follows:

```
SDMB360 mmmdd hh:mm:ss ssdd TBL SDM BILLING COMMS
STREAM=<stream>:
<file transfer mode> - <error msg>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
stream	variable	Identifies the stream where the problem occurred.
file transfer mode	IFT, OFT	Indicates the file transfer mode: Inbound or Outbound.
error msg	constant	Connection to File Client Unavailable

Action

Contact the next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDMB615

The SuperNode Data Manager Billing (SDMB) subsystem generates log SDMB615 when a software-related error condition has been resolved.

Format

The log report format for SDMB615 is as follows:

```
SDMB615 mmmdd hh:mm:ss ssdd INFO SDM BILLING SOFT
ERROR STREAM=<stream>:<status>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
stream	4-character alphanumeric	Identifies the stream to which the log applies.
status	48-character alphanumeric	Provides status information.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDMB660

The SuperNode Data Manager Billing (SDMB) subsystem generates log SDMB660 when a problem involving communications with other SuperNode Billing Application (SBA) features is resolved. This log is associated with the alarm FTP.

Format

The log report format for SDMB660 is as follows:

```
SDMB660 mmmdd hh:mm:ss ssdd INFO SDM BILLING COMMS
STREAM=<stream>:OFT - <specific resolution>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
stream	variable	Identifies the stream where the problem occurred.
specific resolution	variable	Indicates the resolution of the communication problem.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SPM625

The SPM625 log report is generated when crossover message channels are not configured for SPMs.

Format

The log report format for SPM625 is as follows:

```
MSH3XAPT     SPM625 mmmdd hh:mm:ss ssdd INFO SPM XOVER
   NonConformity Report
   This office has 2 SPMs that do not have crossover
   message channels configured.

   Crossover message channel configuration is
   recommended for all DS-512 connected SPMs.
   Please refer to Crossover Messaging IM 65-7644 or
   contact the next level of support.

   The following nodes are not in message channel
   crossover mode:
   SPM 8    SPM 9
```

Selected field descriptions

This log report has no selected field descriptions.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SPM710

The SPM710 log report is generated when the audit updates the ISDNPROT table.

Format

The log report format for SPM710 is as follows:

```
SPM710 mmmdd hh:mm:ss ssdd NONE INFO ISDNPROT Table
update for SPM <spmno>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
spmno	1 through 64	Identifies the node number of the SPM.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

TMN301

Log Report TMN301 is generated when an application error is detected.

Format

The log report format for TMN301 is as follows:

```
May 19 15:48:17 <Machine> syslog: TMN301 <Severity>
TBL Application error
Status: Trouble raised
Location: <software_entity> <user (process id)>
Description: <description>
Action: <action>
```

Note: This example is in syslog format. Your format may differ.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Machine	Variable	Indicates the name of the machine with the problem.
Severity	Critical, Major, or Minor	Indicates the severity of the alarm.
software_entity	Variable	Indicates the location of the problem software entity.
user (process id)	Variable	Indicates the process ID number.
description	Variable	Describes the error.
action	Variable	Indicates the action to take.

Action

The action will vary, depending on the error. Refer to the log report for the specific action to take.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

TMN302

Log Report TMN302 is generated when a system error occurs.

Format

The log report format for TMN302 is as follows:

```
May 19 15:48:17 <Machine> syslog: TMN302 <Severity>
TBL System error
Status: Trouble raised
Location: <software_entity> <user (process id)>
Description: <description>
Action: <action>
```

Note: This example is in syslog format. Your format may differ.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Machine	Variable	Indicates the name of the machine with the problem.
Severity	Critical, Major, or Minor	Indicates the severity of the alarm.
software_entity	Variable	Indicates the location of the problem software entity.
user (process id)	Variable	Indicates the process ID number.
description	Variable	Describes the error.
action	Variable	Indicates the action to take.

Action

The action will vary, depending on the error. Refer to the log report for the specific action to take.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

TMN303

Log Report TMN303 is generated when a communication error occurs.

Format

The log report format for TMN303 is as follows:

```
comp5iems ***  TMN303  FEB14 15:48:17 4635 CBSY
        Communication error
        Location: Normalization Layer maint (33344)
        Description: store is disconnected
        Action: Check Archive Process
```

Selected field descriptions

This log report has no selected field descriptions.

Action

The action will vary, depending on the error. Refer to the log report for the specific action to take.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

TMN304

Log Report TMN304 is generated when a connection error occurs.

Format

The log report format for TMN304 is as follows:

```
May 19 15:48:17 <Machine> syslog: TMN304 <Severity>
TBL Connection error
Status: Trouble raised
Location: <software_entity> <user (process id)>
Description: <description>
Action: <action>
```

Note: This example is in syslog format. Your format may differ.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Machine	Variable	Indicates the name of the machine with the problem.
Severity	Critical, Major, or Minor	Indicates the severity of the alarm.
software_entity	Variable	Indicates the location of the problem software entity.
user (process id)	Variable	Indicates the process ID number.
description	Variable	Describes the error.
action	Variable	Indicates the action to take.

Action

The action will vary, depending on the error. Refer to the log report for the specific action to take.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

TMN309

Log Report TMN309 is generated when a data server error occurs.

Format

The log report format for TMN309 is as follows:

```
May 19 15:48:17 <Machine> syslog: TMN309 <Severity>
TBL Data Server error
Status: Trouble raised
Location: <software_entity> <user (process id)>
Description: <description>
Action: <action>
```

Note: This example is in syslog format. Your format may differ.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Machine	Variable	Indicates the name of the machine with the problem.
Severity	Critical, Major, or Minor	Indicates the severity of the alarm.
software_entity	Variable	Indicates the location of the problem software entity.
user (process id)	Variable	Indicates the process ID number.
description	Variable	Describes the error.
action	Variable	Indicates the action to take.

Action

If the problem persists, contact the next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

TMN311

Log Report TMN311 is generated when a fatal error occurs.

Format

The log report format for TMN311 is as follows:

```
comp5iems *** TMN311 May19 15:48:17 3090 CBSY Fatal
       error
       Location: Log List Server maint (28374)
       Description: Connection with llClient lost
       Action: check llClient
```

Selected field descriptions

This log report has no selected fields.

Action

The action will vary, depending on the error. Refer to the log report for the specific action to take.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

TMN600

Log Report TMN600 is generated by Log Normalizer when the normalizer process is successfully started and when delrep messages are sent successfully to the SDM OSF server.

Format

The log report format for TMN600 is as follows:

```
comp5iems   TMN600 FEB14 10:58:01 0159 INFO
         Information only
         Location: DAL maint(24540)
         Description: Failure to decode OM
         tuple: group = TOPQOCPS, tuple number = 0
```

Selected field descriptions

This log report has no selected field descriptions.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

TMN601

Log Report TMN601 is generated if the version summary file is not found, meaning that the archive is empty. It is normal for the version summary file to not be found when the archive process is started for the first time.

Format

The log report format for TMN601 is as follows:

```
May 19 15:48:17 <Machine> syslog: TMN601 NONE INFO
File IO info
Location: <software_entity> <user (process id)>
Description: <description>
```

Note: This example is in syslog format. Your format may differ.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Machine	Variable	Indicates the name of the machine.
software_entity	Variable	Indicates the location of the software entity.
user (process id)	Variable	Indicates the process ID number.
description	Variable	Describes the process or the error.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

TMN604

Log Report TMN604 is generated to provide information about application status.

Format

The log report format for TMN604 is as follows:

```
comp5iems   TMN604 FEB14 11:30:01 2979 INFO
        Application status
        Location: rscReporter root (nodes:15368)
        Description: Connection to Process Control is
        re-established.
```

Selected field descriptions

This log report has no selected field descriptions.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

TMN605

Log Report TMN605 is generated to provide Core restart information.

Format

The log report format for TMN605 is as follows:

```
comp5iems  FEB10 16:12:47 3708 INFO Core Restart Info
Location: <software_entity> <user (process ID)>
Description: Last restart type: <type>, last restart
time :
<yyyy/mm/dd HH:MM:SS.000 A>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
type	• warm restart • cold restart • reload restart • warm swact • cold swact • norestart swact • abort swact • unknown	Indicates the type of Core restart.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

AMS300

Log report AMS300 indicates a board reset on the Media Server 2000 node. The IPM-1610 or TP-6310 board was reset.

Format

Reset Board - associated trap is <acBoardEvResettingBoard>

Selected field descriptions

This log report has no selected fields.

Action

There is no corresponding clear SNMP trap. The status stays critical until a reboot and a board started trap occurs.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

AMS301

Log report AMS301 indicates a fatal error the Media Server 2000 node. The IPM-1610 or TP-6310 board has an un-recoverable run-time error.

Format

Fatal Error - associated trap is <acBoardFatalError>

Selected field descriptions

This log report has no selected fields.

Action

Check alarms and additional logs to determine the reason for the failure.

Associated OM registers

This log report has no associated OM registers.

Additional information

There is no corresponding clear SNMP trap. The status stays critical until a reboot.

AMS302

Log report AMS302 indicates a configuration error on the Media Server 2000 node. There is an error in the current configuration for the Media Server 2000 Series node.

Format

Configuration Error - associated trap is <acBoardConfigurationError>

Selected field descriptions

This log report has no selected fields.

Action

Check alarms and additional logs to determine the reason for the failure.

Associated OM registers

This log report has no associated OM registers.

Additional information

There is no corresponding clear SNMP trap. The status stays critical until a reboot.

AMS303

Log report AMS303 indicates a temperature alarm. The MS 2000 Series node has a higher than normal temperature condition. This alarm trap is sent from the server when the temperature is above 60 degrees C (140 degrees F).

Format

Temperature Alarm - associated trap is <acBoardTemperatureAlarm>

Selected field descriptions

This log report has no selected fields.

Action

Determine the reason for the high temperature in the Media Server 2000 node.

Associated OM registers

This log report has no associated OM registers.

Additional information

The status stays critical until a corresponding alarm clear is sent when the temperature falls below 55 degrees C (131 degrees F).

AMS304

Log report AMS304 indicates a feature key error on the Media Server 2000 node. The use of a service (such as conferencing, voice prompts) was attempted but a feature key allowing use of the service was not found.

Format

Feature Key Error - associated trap is <acFeatureKeyError>

Selected field descriptions

This log report has no selected fields.

Action

Check the configuration and correct if necessary.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

AMS305

Log report AMS305 indicates board call resource alarm on the Media Server 2000 node. This alarm is raised only in SIP/H.323-based gateway products as a major alarm.

Format

Board Call Resource Alarm - associated trap is <acBoardCallResourceAlarm>

Selected field descriptions

This log report has no selected fields.

Action

Check alarms and additional logs to determine the reason for the failure.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

AMS306

Log report AMS306 indicates a board controller failure alarm on the Media Server 2000 node. This alarm is raised only in SIP/H.323-based gateway products as a minor alarm.

Format

Board Controller Failure - associated trap is <acBoardControllerFailureAlarm>

Selected field descriptions

This log report has no selected fields.

Action

Check alarms and additional logs to determine the reason for the failure.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

AMS307

Log report AMS307 indicates an ethernet link alarm on the Media Server 2000 node. This alarm trap is received when there is a fault on one of the ethernet links which has an alarm status of “major”. If there is a fault on both interfaces, the alarm status is critical and the server is isolated.

Format

Ethernet Link Alarm - associated trap is <acBoardEthernetLinkAlarm>

Selected field descriptions

This log report has no selected fields.

Action

When both link interfaces are restored, an SNMP alarm clear trap is sent and the alarm is cleared.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

AMS308

Log report AMS308 indicates a board overload on the Media Server 2000 node. This alarm is raised only in SIP/H.323-based gateway products as a major alarm.

Format

Overload Alarm - associated trap is <acBoardOverloadAlarm>

Selected field descriptions

This log report has no selected fields.

Action

Check alarms and additional logs to determine the reason for the failure.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

AMS309

Log report AMS309 indicates an active alarm table overflow on the Media Server 2000 node. During each development cycle, a calculation is made as to the size of the active alarm table that will hold all possible alarms that can be raised at any one time by the board. This alarm will only be seen if there is an error in that calculation.

Format

Active Alarm Table Overflow - associated trap is <acActiveAlarmTableOverflow>

Selected field descriptions

This log report has no selected fields.

Action

The status stays major until reboot, because it denotes a possible loss of information until the next reboot.

Associated OM registers

This log report has no associated OM registers.

Additional information

If an alarm was raised when the table was full, it is possible that the alarm is active, but does not appear in the active alarm table.

AMS310

Log report AMS310 indicates an ATM port alarm on the Media Server 2000 node. This is applicable for the MS2020 server and indicates an ATM port error.

Format

Atm Port Alarm - associated trap is <acAtmPortAlarm>

Selected field descriptions

This log report has no selected fields.

Action

Check alarms and additional logs to determine the reason for the failure.

Associated OM registers

This log report has no associated OM registers.

Additional information

The status stays critical until the problem is resolved and a reboot occurs.

AMS311

Log report AMS311 indicates an audio provisioning alarm on the Media Server 2000 node. An audio provisioning alarm trap is sent when the AMS times out waiting for audio provisioning from the audio provisioning server.

Format

Audio Provisioning Alarm - associated trap is <acAudioProvisioningAlarm>

Selected field descriptions

This log report has no selected fields.

Action

Check alarms and additional logs to determine the reason for the failure.

Associated OM registers

This log report has no associated OM registers.

Additional information

A clear alarm trap is sent when a successful audio provisioning session occurs.

AMS312

Log report AMS312 indicates an operational state change on the Media Server 2000 node to “disabled”. When the state changes from enabled to disabled, an SNMP traps is sent with a “major” status. If the MS2000 (ATM or IP) fails to initialize the operation state is disabled.

Format

Operational State Change - associated trap is <acOperationalStateChange>

Selected field descriptions

This log report has no selected fields.

Action

Check alarms and additional logs to determine the reason for the failure.

Associated OM registers

This log report has no associated OM registers.

Additional information

A corresponding clear trap is sent when the state changes back to an “enabled” state. In ATM systems, the operational state of the node is also disabled if there are no ATM ports available for use. An ATM port is available for use if it is unlocked and enabled.

AMS501

Log report AMS501 indicates an admin state change on the Media Server 2000 node. The administration state of the MS 2000 Series node changed either to “locked”, “shutting down“, or “unlocked“.

Format

Admin State Change - associated trap is <acgwAdminStateChange>

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

An MS 2000 Series node can be locked gracefully, allowing existing calls to complete, before administration (configuration and maintenance) is performed on the node. The MS2000 Series also supports a forced lock which immediately takes down active calls. In both types of locks, the administrative state changes to critical for either a “shutting down” or “locked” state and clears when it transitions to an unlocked state.

SPCM300

Log report SPCM300 is a Policy Controller Maintenance Trouble information log. It is generated by the Policy Controller application maintenance process for a variety of unexpected reasons or conditions which may include:

- messaging failures
- failure to set a timer
- timer expirations that should not occur
- failure to write to the “SA_State” file
- process deaths
- failure to start the callp process

The Policy Controller application generates log report SPCM300 in addition to raising the SPCM300 alarm.

Format

The format for log report SPCM300 is as follows:

```
Apr 6 13:24:47 SPC6-Unit1 spcappmtc: SPCM300 NONE TBL SPC Application
Maintenance Trouble
{Reason Text : Application process death]
[Error Code  : -1]
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	spcappmtc	Identifies the NGCL or application process unit that generates the report
Log Number	SPCM300	The component prefix and number of the log

Field	Value	Description
Severity	None	The log severity (may be related to alarm severity)
Event Type	TBL (trouble)	The type of trouble or info recorded; this is an information only log
Label	SPC Maintenance Trouble	Title label for the log
Description	Reason text	Detailed description of the trouble or activity; see section Additional Information for a detail list of Trouble reasons

Action

No action is required. This is an information log only.

Associated OM registers

This log report has no associated OM registers.

Additional information

The following additional information applies to the Description field of the log entry:

- [Reason Text: <TroubleReason>]
  - SAM to Web Server message send failure
  - SAM to Policy Controller CallP message send failure
  - Been Terminating too long. Timer Expired.
  - SAM Wait Timer Messaging Timeout
  - SAM/Policy Controller CallP Audit Messaging Timeout
  - Failed to set the Policy Controller Application state
  - Policy Controller Application process death
  - Failed to start the Policy Controller Application process
  - Failed to set a timer
  - Policy Controller CallP created, but not in the requested state
  - Policy Controller CallP created, but failed to reply to SAM
  - Policy Controller CallP on the Inactive failed to respond to a request

- Policy Controller CallP on the Inactive failed to get to the requested state
- SAM failed to send a reply to a platform swact request
- SAM failed a Swact Request due to an invalid Swact Request
- SAM failed a Graceful Swact Request due to being marked to do a COLD Swact
- SAM failed a Swact Precheck Request due to option = FORCE
- SAM failed a Swact Precheck or PreSwact request due to option = NOW
- SAM failed a Swact Request due to an invalid option
- SAM failed a Swact Request due to an unacceptable platform status
- SAM failed a Swact Request due to not being In-Sync
- Swact Precheck Failed due to failure received in Policy Controller CallP response
- Swact Precheck Failed due to failure to notify Policy Controller CallP
- Swact Precheck Failed due to timeout waiting on Policy Controller CallP response
- Swact PreSwact Failed due to failure received in Policy Controller CallP response
- Swact PreSwact Failed due to failure to notify Policy Controller CallP
- Swact PreSwact Failed due to timeout waiting on Policy Controller CallP response
- Swact AbortSwact Failed due to failure received in Policy Controller CallP response
- Swact AbortSwact Failed due to failure to notify Policy Controller CallP
- Swact AbortSwact Failed due to timeout waiting on Policy Controller CallP response
- Swact PostSwact Failed due to failure received in Policy Controller CallP response
- Swact PostSwact Failed due to failure to notify Policy Controller CallP
- Swact PostSwact Failed due to timeout waiting on Policy Controller CallP response

- Disable PreCheck Failed due to failure received in Policy Controller CallP response
- Disable PreCheck Failed due to timeout waiting on Policy Controller CallP response
- Disable PreDisable Failed due to failure received in Policy Controller CallP response
- Disable PreDisable Failed due to timeout waiting on Policy Controller CallP response
- Disable AbortDisable Failed due to failure received in Policy Controller CallP response
- Disable AbortDisable Failed due to timeout waiting on Policy Controller CallP response
- Swact PreSwact Failed due to failure to notify Policy Controller CallP
- Disable PreDisable Failed due to failure received from the mate SAM
- Disable PreDisable Failed due to failure to notify Policy Controller CallP
- Disable PreDisable Failed due to timeout waiting on mate SAM response
- Disable AbortDisable Failed due to failure received from the mate SAM
- Disable AbortDisable Failed due to failure to notify Policy Controller CallP
- Disable AbortDisable Failed due to timeout waiting on mate SAM response
- Disable Request Failed due to Callback called with existing disable request outstanding
- Disable Request Failed due to Callback called when platform not active and enabled
- Disable Inactive Failed due to Callback called when platform not in duplex
- Disable Inactive PreCheck Failed due to Callback called when SAM had a conflicting wait state
- Disable Inactive PreDisable Failed due to Callback called when SAM had a conflicting wait state
- Disable Inactive AbortDisable Failed due to Callback called when SAM had a conflicting wait state

- — Disable PreCheck Failed due to failure to notify Policy Controller CallP
- — Disable PreDisable Failed due to failure to notify the Mate SAM
- — Disable AbortDisable Failed due to failure to notify the Mate SAM
- — Disable Active Failed due to Callback called when platform was in duplex
- — Disable Active Graceful Failed due to Callback called when Policy Controller State was not suspended
- — Disable Callback called with invalid request
- — SAM received a response to a Swact request that contained an invalid request
- — SAM received a response to a Swact request that contained an invalid option
- — SAM received a response to a Swact request that contained an invalid result
- — Mate SAM failed a Prepare For COLD Swact request, reverting to a WARM swact
- — Failed to notify the Mate SAM to Prepare For COLD Swact request, reverting to a WARM swact
- — Timed out waiting on the Mate SAM to respond to a Prepare For COLD Swact request, reverting to a WARM swact
- — SAM failed to register with DataSync

• <ErrorCode>: This is an integer code used for debugging. -1 is the default value

SPCM301

Log report SPCM301 generated when its associated critical alarm is raised because the Policy Controller Application has transitioned to a state that indicates it should be in-service, but is actually not, while the active Policy Controller unit running the Policy Controller application is in an enabled operational state. This “system busied” (SYSB) state is represented by state values as follows:

- Administrative State = Unlocked
- Operational State = Disabled
- Procedural Status = “-” or Not Terminating
- Control Status = “-” or Not Suspended

Call processing cannot occur while the Policy Controller application is in this state.

The Policy Controller application generates log report SPCM301 in addition to raising or clearing the alarm.

Format

The format for log report SPCM301 is as follows:

```
Dec 22 16:20:24 PV-SPC6-0 alarmd: SPCM301 CRIT TBL NGSS App Maintenance
Trouble Alarm : NCGL=PV-SPC6-0;Unit=0; SPC Application System Busy
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	SPCM301	The component prefix and number of the log

Field	Value	Description
Severity	Critical or None	The log severity (may be related to alarm severity)
Event Type	TBL (trouble)	The type of trouble or info recorded
Label	NGSS Maintenance Trouble Alarm	Title label for the log
DeviceInfo	Alphanumeric	Info that specifies the device to which the alarm pertains
AlarmRaiseLowerText	Alphanumeric	Text indicating whether the Policy Controller Application System Busy alarm has been raised or cleared

Action

When the Policy Controller Application transitions out of this state (automatically or manually), this alarm is lowered. It is also lowered if the Policy Controller unit the application is running on leaves the enabled operational state.

When this alarm is raised, the system attempts recovery immediately. If immediate recovery is not successful, reattempts are made automatically every 30 seconds.

A manual method to attempt recovery from this alarm condition can be performed by executing the following procedures in order, found in the *Policy Controller Security and Administration NTP, NNxxxxx-611*:

- Perform procedure *Lock the Policy Controller application*
- Perform procedure *Unsuspend the Policy Controller application*
- Perform procedure *Unlock the Policy Controller application*

If the alarm condition persists, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SPCM302

Log SPCM302 is generated by a major alarm that is raised when the Policy Controller platform that the Policy Controller Application is running on is in a duplex configuration with both units in an enabled operational state, and the Policy Controller application state goes out of sync between the two Policy Controller units.

This alarm is cleared if the Policy Controller application state becomes sync'ed between the two Policy Controller units and the alarm is cleared.

Format

The format for log report SPCM302 is as follows:

```
Dec 22 16:20:24 PV-SPC6-0 alarmd: SPCM302 MAJOR TBL NGSS App Maintenance
Sync Trouble Alarm : NCGL=PV-SPC6-0;Unit=0; SPC Application Mtc Out
Of Sync
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	SPCM302	The component prefix and number of the log
Severity	Major or None	The log severity (may be related to alarm severity)
Event Type	TBL (trouble)	The type of trouble or info recorded
Label	NGSS Maintenance Trouble Alarm	Title label for the log

Field	Value	Description
DeviceInfo	Alphanumeric	Info that specifies the device to which the alarm pertains
AlarmRaiseLowerText	Alphanumeric	Text indicating whether the Policy Controller Application Mtc Out Of Sync alarm has been raised or cleared

Action

The Policy Controller application should attempt to sync itself automatically every 30 seconds. If there repeated sync failures, a manual method to attempt recovery from this alarm condition can be performed by executing the following procedures in order, found in the *Policy Controller Security and Administration NTP, NN10434-611*:

- Perform procedure *Lock the Policy Controller application*
- Perform procedure *Suspend the Policy Controller application*
- Perform procedure *Unsuspend the Policy Controller application*
- Perform procedure *Unlock the Policy Controller application*

If the alarm condition persists, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SPCM500

Log report SPCM500 is a SIP Maintenance State Change information log. The state of the SIP Application is actually updated by the callp process, but, the SIP Application maintenance message handler process thread keeps track of the last known state. When a message is received from callp, the SIP application maintenance process, running on the Policy Controller, checks to see if the current state matches the last known state. If it does not, then a state change log is generated. If the SIP application maintenance process updates the state, it also generates a state change log at the same time.

The Policy Controller application generates log report SPCM500 in addition to raising the associated alarm.

State change logs include content indicated the FROM and TO states in external format, an indication of whether a user requested the change (if it was not system generated), a reason for the change, and a userid of the user that requested the change.

Format

The format for log report SPCM500 is as follows:

```
Feb 4 11:28:22 spc6-Unit1 spcappmtc: SPCM500 NONE INFO SPC Application
Maintenance State Change [Administrative : Locked -> Locked ]
[Operational : Disabled -> Enabled ] [Control : Suspended -> Not
Suspended ] [Procedural : Not Terminating -> Not Terminating] [User
Requested : No] [Reason : System originated change of state] [Web User
ID : ]
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID or device name	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	spcappmtc	Identifies the NGCL or application process unit that generates the report

Field	Value	Description
Log Number	SPCM500	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	SPC Maintenance State Change	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity; see section: Additional information on page 175

Action

No action is required. This is an information log only.

Associated OM registers

This log report has no associated OM registers.

Additional information

The following additional information applies to the Description field of the log entry:

- [Administrative: <AdminFrom> -> <AdminTo>]
  - Locked
  - Unlocked
  - Shutting down
- [Operational: <OperFrom> -> <OperTo>]
  - Enabled
  - Disabled
- [Control: <CtrlFrom> -> <CtrlTo>]
  - Suspended
  - Not Suspended
- [Procedural: <ProcFrom> -> <ProcTo>]
  - Terminating
  - Not Terminating
- [User Requested: <Yes|No>]
  - Yes
  - No
- [Reason: <StateChangeReason>]
  - Unsuspend command issued
  - Suspend command issued
  - Lock command issued
  - Lock command in progress
  - Lock operation complete
  - Unlock command issued
  - Shut Down command issued
  - Shut Down operation complete
  - System originated change of state
  - Timeout waiting to terminate call processing
  - Audit Failure
  - Timer Problem
  - Data corruption detected

- [Web User ID: <webuserid>]
  - If applicable, this is the web interface login ID of the user performing the maintenance that caused the state transition. If not applicable, this value is left blank. Refer to the *Overview* section of the *Policy Controller Security and Administration NTP, NNxxxxx-611* for information about login IDs and user IDs and authorization categories

SPCP301

Log report SPCP301 indicates that the Policy Controller application server signaling interface has a communication failure.

Format

The format for log report SPCP301 is as follows:

```
Apr 15 16:12:13 spc1 alarmd: SPCP301 MAJOR TBL AppServer Signaling
Communication Failure NCGL=spc1;Unit=0;SPCP AppServer 47.153.178.146
Signaling Communication Failure
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	spccallp	Identifies the NGCL or application process unit that generates the report
Log Number	SPCP301	The component prefix and number of the log
Severity	MAJOR	The log severity (may be related to alarm severity)
Event Type	TBL	This is an informational log
Label	AppServer Signaling Communication Failure	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

Check the application server status and the link to the application server.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

SPCP302

Log report SPCP302 indicates that the Policy Controller has lost database connection.

Format

The format for log report SPCP302 is as follows:

```
Apr 13 12:13:27 spc1 alarmd: SPCP302 CRIT TBL No Database Connection
NCGL=spc1;Unit=0;SPCP SPC Processing No Database Connection
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	SPCP302	The component prefix and number of the log
Severity	CRIT	The log severity (may be related to alarm severity)
Event Type	TBL	This is an informational log
Label	No Database Connection	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

SPCP303

Log report SPCP303 indicates that the Application server request failure ratio exceeds the predefined threshold value.

Format

The format for log report SPCP303 is as follows:

```
Apr 13 12:23:43 spc1 alarmd: SPCP303 MINOR TBL  CAC Request Mass Failure
NCGL=spc1;Unit=0;SPCP CAC Request Failure Exceed Threshold
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	SPCP303	The component prefix and number of the log
Severity	MINOR	The log severity (may be related to alarm severity)
Event Type	TBL	This is an informational log
Label	CAC Request Mass Failure	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

SPCP304

Log report SPCP304 indicates that the Policy Controller Endpoint Number exceeds the Endpoint Block Size.

Format

The format for log report SPCP304 is as follows:

```
Apr 13 17:26:02 spc1 alarmd: SPCP304 CRIT TBL  Exceed Endpoint Block Size
NCGL=spc1;Unit=0;SPCP Endpoint Number Exceed Endpoint Block Size
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	SPCP304	The component prefix and number of the log
Severity	CRIT	The log severity (may be related to alarm severity)
Event Type	TBL	This is an informational log
Label	Exceed Endpoint Block Size	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

Obtain a new license to enlarge the endpoint number supported

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

SPCP305

Log report SPCP305 indicates that the Policy Controller Endpoint Number exceeds the Endpoint Block Warning Size.

Format

The format for log report SPCP305 is as follows:

```
Apr 14 17:36:02 spc1 alarmd: SPCP305 MAJOR TBL  Exceed Endpoint Block
Warning Size NCGL=spc1;Unit=0;SPCP Endpoint Number Exceed Endpoint Block
Warning Size
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	SPCP305	The component prefix and number of the log
Severity	MAJOR	The log severity (may be related to alarm severity)
Event Type	TBL	This is an informational log
Label	Exceed Endpoint Block Warning Size	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

Obtain a new license to enlarge the endpoint number supported.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

SPCP501

Log report SPCP501 indicates that the Policy Controller application has started up.

Format

The format for log report SPCP501 is as follows:

```
APR17 08:04:43 SPC2-Unit1 spccallp: SPCP501 NONE INFO SPC Startup
SPC start up successfully
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	spccallp	Identifies the NGCL or application process unit that generates the report
Log Number	SPCP501	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	This is an informational log
Label	SPC Startup	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

SPCP502

Log report SPCP502 indicates that the Policy Controller application has shut down.

Format

The format for log report SPCP502 is as follows:

```
APR17 08:04:43 SPC1-Unit1 spccallp: SPCP501 none INFO SPC Shutdown
SPC shut down successfully
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	spccallp	Identifies the NGCL or application process unit that generates the report
Log Number	SPCP502	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	This is an informational log
Label	SPC Shutdown	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

SPCP601

Log report SPCP601 indicates that a Flow Status Audit has completed.

Format

The format for log report SPCP601 is as follows:

```
APR17 08:04:43 SPC2-Unit1 spcallp: SPCP601 none INFO Audit Result
StatusAck Message is received, Flow 256 still exists
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	spccallp	Identifies the NGCL or application process unit that generates the report
Log Number	SPCP601	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	This is an informational log
Label	Audit Result	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

SPCP602

Log report SPCP602 indicates that a CAC request from the application server has been denied.

Format

The format for log report SPCP602 is as follows:

```
APR17 08:04:43 SPC1-Unit1 spccallp: SPCP602 none INFO CAC Request Denied
Commit Message: Gate 1908 from GWC 47.153.178.146 is not found in SPC
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	spccallp	Identifies the NGCL or application process unit that generates the report
Log Number	SPCP602	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	This is an informational log
Label	CAC Request Denied	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

The following OMs are pegged:

- SPC Reservation Request or SPC Commit Request
- CAC Request on Network Segment

Additional information

This log report has no additional information.

SPCP603

Log report SPCP603 indicates that a the Policy Controller callp has accepted a topology change.

Format

The format for log report SPCP603 is as follows:

```
APR17 08:04:43 SPC1-Unit1 spccallp: SPCP603 none INFO Topology Change
Topology Notify AddNode [NZID: 2] successfully
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	spccallp	Identifies the NGCL or application process unit that generates the report
Log Number	SPCP603	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	This is an informational log
Label	Topology Change	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

None

Additional information

This log report has no additional information.

SPCP604

Log report SPCP604 indicates that callP has detected that the Ingress Id of the Network Segment sent in a GateSet message from the GWC is not present in the Policy Controller database. This is an indication that there could be a topology mismatch between the Policy Controller and the GWC/SESM. A summary of the requested problem is included in the free text portion of the report decription field.

Format

The format for log report SPCP604 is as follows:

```
APR17 08:04:43 SPC1-Unit1 spccallp: SPCP604 none INFO Topology Mismatch
Reserve Message: Network Zone 6 from GWC 47.142.130.104 does not exist
in SPC Topology
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	spccallp	Identifies the NGCL or application process unit that generates the report
Log Number	SPCP604	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	This is an informational log
Label	Topology Mismatch	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

None

Additional information

This log report has no additional information.

TPM301

Log report TPM301 indicates that the Topology Manager has lost database connection.

Format

The format for log report TPM301 is as follows:

```
Apr 14 12:01:59 spc1 alarmd: TPM301 CRIT TBL  No Database Connection
NCGL=spc1;Unit=0;TPM Topology Manager No Database Connection
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	TPM301	The component prefix and number of the log
Severity	CRIT	The log severity (may be related to alarm severity)
Event Type	TBL	This is an informational log
Label	No Database Connection	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

TPM501

Log report TPM501 indicates that the Topology Manager application has started up.

Format

The format for log report TPM501 is as follows:

```
APR17 08:04:43 SPC2-Unit1 spctm: TPM501 none INFO TopologyManager startup
Server Startup
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	spccallp	Identifies the NGCL or application process unit that generates the report
Log Number	TPM501	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	This is an informational log
Label	Topology Manager startup	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

None

Additional information

This log report has no additional information.

TPM502

Log report TPM502 indicates that the Topology Manager application has shut down.

Format

The format for log report TPM502 is as follows:

```
APR17 08:04:43 SPC2-Unit1 spctm: TPM502 none INFO TopologyManager shutdown
server will exit after receiving RESTART command or signal.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	spccallp	Identifies the NGCL or application process unit that generates the report
Log Number	TPM502	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	This is an informational log
Label	Topology Manager shutdown	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

None

Additional information

This log report has no additional information.

TPM601

Log report TPM601 indicates that the Topology Manager application has accepted a topology change. A summary of the requested change is includes in the free text portion of the report decription field.

Format

The format for log report TPM601 is as follows:

```
APR17 08:04:43 SPC2-Unit1 spctm: TPM601 none INFO Topology Change
User(mtc) add NetworkZone(NZID:3 Name:test.1) success!
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	spccallp	Identifies the NGCL or application process unit that generates the report
Log Number	TPM601	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	This is an informational log
Label	Topology Change	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

None

Additional information

This log report has no additional information.

CRTM700

Log report CRTM700, titled *New private key requested*, is generated during the execution of the Certificate Management Tool , when either option 1 (generate a self-signed certificate) or option 2 (generate a certificate signing request) is used. Using either option 1 or 2 backs up the existing private key within the /opt/base/share/ssl directory and any new private key generated is placed in file /opt/base/share/ssl/server.key. This is an information log only and is not associated with an alarm.

Format

The format for log report CRTM700 is as follows:

```
Nov 11 14:12:14 ngss.unit0 cert_mgnt: CRTM700 NONE INFO CERT_MGNT
User requested new private key.
Existing key moved to /opt/base/share/ssl/server.key.1412_11112004
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	cert_mgnt	Identifies the NGCL or application process unit that generates the report
Log Number	CRTM700	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	The type of trouble or info recorded
Label	cert_mgnt	Title label for the log
Description	User requested new private key	Detailed description of the trouble or activity

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Use the Certificate Management Tool screen output and TLS initialization logs to ensure that the new key and certificate were provisioned properly.

CRTM701

Log report CRTM701, titled, *Self signed certificate requested*, is generated during the execution of the Certificate Management Tool, option 1, (generate a self-signed certificate). Self-signed certificates carry a security risk because they are not signed by a trusted certificate authority (CA) and therefore cannot be authenticated by a certificate authority. This information log is a notification that the user accepted the disclaimer regarding the risks associated with using self-signed certificates. No alarms are associated with this log.

Format

The format for log report CRTM701 is as follows:

```
Nov 12 09:54:50 comit.ngss.unit0 cert_mgnt: CRTM701 NONE INFO CERT_MGNT
User accepted disclaimer for generating self-signed certificates
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	cert_mgnt	Identifies the NGCL or application process unit that generates the report
Log Number	CRTM701	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	The type of trouble or info recorded

Field	Value	Description
Label	CERT_MGNT	Title label for the log
Description	User accepted disclaimer for generating self-signed certificates	Detailed description of the trouble or activity

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Use the Certificate Management Tool screen output and TLS initialization logs to ensure that the new key and certificate were provisioned properly.

DBSE300

Log report DBSE300 is generated any time a change in database connectivity is detected, specifically a loss of connectivity between the Session Server or Policy Controller provisioning watchdog program and the Solid database. It reports 'No Solid DB Connection' when database connectivity is lost and a critical "No Database Connection Alarm" is raised.

DBSE300 reports 'Solid DB Connection Restored' when database connectivity is reestablished and the critical "No Database Connection Alarm" is cleared.

Format

The format for log report DBSE300 is as follows:

```
Mar 22 21:27:48 vm0 alarmd:DBSE300 CRIT TBL No Solid DB Connection No
Database Connection

Mar 22 21:27:48 vm0 alarmd:DBSE300 CRIT TBL Solid DB Connection Restored
No Database Connection
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	DBSE300	The component prefix and number of the log
Severity	critical	The log severity (may be related to alarm severity)
Event Type	TBL (trouble)	The type of trouble or info recorded

Field	Value	Description
Label	Alphanumeric	Title label for the log
Description	No Database Connection	Detailed description of the trouble or activity or activity

Action

Take corrective action to restore the unresponsive database.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SIPC301

Log report SIPC301 titled *All Incoming SIP Msgs Blocked* is a critical log that is generated when the SIP Gateway Call Processing Application does not receive any incoming SIP messages due to Access Control List (ACL) being enabled and no valid entries in Remote SIP server or ACL.

Format

The format for log report SIPC301 is as follows:

```
Nov 12 21:32:08 loopback sipgwyappln: SIPC301 CRIT TBL All SIP Incoming
Msgs Blocked
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPC301	The component prefix and number of the log
Severity	Critical	The log severity (may be related to alarm severity)
Event Type	TBL (trouble)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	All SIP Incoming Msgs Blocked	Detailed description of the trouble or activity or activity

Action

No action is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SIPC310

Log report SIPC310 is generated for the following alarm conditions

- indicates that “SIP CallP No Database Connection” is associated with the generation of the critical alarm due to a loss of connectivity between the SIP Gateway application database and the CallP application.
- indicates the SIP Gateway application crossing an overload threshold. The logs are used, along with an associated major alarm to indicate overload control status.

Format

The format for log report SIPC310 is as follows:

```
Sep 13 19:20:14 cablab.ss.unit0 alarmd: SIPC310 CRIT TBL SIP CallP
NCGL=cablab.ss.unit0;Unit=0;SIPC No Database Connection

Sep 13 19:20:14 cablab.ss.unit0 alarmd: SIPC310 NONE TBL SIP CallP
NCGL=cablab.ss.unit0;Unit=0;SIPC Automatically cleared due to alarm
generator process death

May  9 13:45:26 rtpfngss1 alarmd: SIPC310 MAJOR TBL  SIP CallP
NCGL=rtpfngss1;Unit=1;SIPC Overload Threshold Reached

Jan 12 13:26:47 RTP7-UNIT1 alarmd: SIPC310 MINOR TBL SIP CallP
NCGL=RTP7-UNIT1;Unit=1;SIPC Overload Condition Pending

Jan 12 13:27:07 RTP7-UNIT1 alarmd: SIPC310 MAJOR TBL SIP CallP
NCGL=RTP7-UNIT1;Unit=1;SIPC Overload Threshold Reached

Jan 12 13:27:17 RTP7-UNIT1 alarmd: SIPC310 NONE TBL SIP CallP
NCGL=RTP7-UNIT1;Unit=1;SIPC Overload Alarm Cleared
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log

Field	Value	Description
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	SIPC310	The component prefix and number of the log
Severity	CRIT, MAJOR, MINOR	The log severity (may be related to alarm severity)
Event Type	TBL or INFO	The type of trouble or info recorded
Label	SIP CallP	Title label for the log
Description	No Database Connection or Overload Threshold Reached	See a detailed description of the trouble in the log details.

Action

Reestablish connectivity between SIP Gateway application process and the database.

For overload conditions, the SIP Gateway application applies flow control to throttle originations. The percentage of originations allowed to complete is indicated in a related STGW700 log report. Existing calls are not affected.

Associated OM registers

If a major alarm/log is generated, indicating an overload threshold is reached, then the associated SIPGW_CALLP OM group OVRLD_CALLS_REJECTED register is incremented. OM group SIPGW_OVERLOAD is also related.

Additional information

This log report requires no additional information.

SIPC550

Log report SIPC550, titled *SIP CallP No Database Connection*, is associated with the generation of the Critical alarm due to a loss of connectivity between the database and the CallP application. A Critical alarm is generated.

A second associated SIPC550 log is labelled *SIP CallP Database Connection Established* when the connection that caused the first SIPC550 log is re-established and the alarm is cleared.

Format

The format for log report SIPC550 is as follows:

```
Nov 12 21:27:48 loopback alarmd:SIPC550 CRIT TBL SIP CallP No Database
Connection: No Database Connection


Nov 12 21:29:34 loopback alarmd:SIPC550 NONE TBL SIP CallP Database
Connection Established: No Database Connection - Alarm Cleared
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	Alphanumeric, ex. alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	SIPC550	The component prefix and number of the log
Severity	Critical or None	The log severity (may be related to alarm severity)
Event Type	TBL (trouble)	The type of trouble or info recorded

Field	Value	Description
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

Establish connectivity between CallP and the Database

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SIPC650

Log report SIPC650, titled *IP CallP No Data Found,* is an informational log that is generated when the SIP Gateway Call Processing Application goes to get data from the database for a particular table and no data is found.

Format

The format for log report SIPC650 is as follows:

```
Nov 12 21:32:08 loopback sipgwyappln: SIPC650 NONE INFO SIP CallP No Data
Found: SIPT GWC
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPC650	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	No Data Found	Detailed description of the trouble or activity

Action

No action is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SIPC750

Log report SIPC750, titled *SIP Access Control List*, is generated when the SIP Gateway Call Processing Application drops incoming SIP messages due to Access Control List restrictions.

A Minor, Major or Critical log is generated based on the number of SIP messages dropped in last 15 minutes:

- Minor Threshold: 25 messages
- Major Threshold: 100 messages
- Critical Threshold: 500 messages

Format

The format for log report SIPC750 is as follows:

```
Nov 12 21:32:08 loopback sipgwyappln: SIPC750 CRIT TBL Incoming 600 SIP
messaged dropped
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPC750	The component prefix and number of the log
Severity	MIN/MAJ/CRIT	The log severity (may be related to alarm severity)
Event Type	INFO	The type of trouble or info recorded

Field	Value	Description
Label	Alphanumeric	Title label for the log
Description	Incoming SIP messages dropped	Detailed description of the trouble or activity

Action

No action is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SIPM300

Log report SIPM300 is a SIP Maintenance Trouble information log. It is generated by the SIP Gateway application maintenance process for a variety of unexpected reasons or conditions which may include:

- messaging failures
- failure to set a timer
- timer expirations that should not occur
- failure to write to the “SA_State” file
- process deaths
- failure to start the callp process

The SIP Gateway application generates log report SIPM300 in addition to raising the SIPM300 alarm.

Format

The format for log report SIPM300 is as follows:

```
Apr 6 13:24:47 RTPF-SIP0 sipgwymtc: SIPM300 NONE TBL SIP Gateway
Maintenance Trouble
{Reason Text : SIP Gateway Application process death]
[Error Code  : -1]
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwymtc	Identifies the NGCL or application process unit that generates the report
Log Number	SIPM300	The component prefix and number of the log

Field	Value	Description
Severity	None	The log severity (may be related to alarm severity)
Event Type	TBL (trouble)	The type of trouble or info recorded; this is an information only log
Label	SIP Gateway Maintenance Trouble	Title label for the log
Description	Reason text	Detailed description of the trouble or activity; see section Additional Information for a detail list of Trouble reasons

Action

No action is required. This is an information log only.

Associated OM registers

This log report has no associated OM registers.

Additional information

The following additional information applies to the Description field of the log entry:

- [Reason Text: <TroubleReason>]
  - SAM to Web Server message send failure
  - SAM to SIP CallP message send failure
  - Been Terminating too long. Timer Expired.
  - SAM Wait Timer Messaging Timeout
  - SAM/SIP CallP Audit Messaging Timeout
  - Failed to set the SIP Gateway Application state
  - SIP Gateway Application process death
  - Failed to start the SIP Gateway Application process
  - Failed to set a timer
  - SIP CallP created, but not in the requested state
  - SIP CallP created, but failed to reply to SAM
  - SIP CallP on the Inactive failed to respond to a request
  - SIP CallP on the Inactive failed to get to the requested state

- SAM failed to send a reply to a platform swact request
- SAM failed a Swact Request due to an invalid Swact Request
- SAM failed a Graceful Swact Request due to being marked to do a COLD Swact
- SAM failed a Swact Precheck Request due to option = FORCE
- SAM failed a Swact Precheck or PreSwact request due to option = NOW
- SAM failed a Swact Request due to an invalid option
- SAM failed a Swact Request due to an unacceptable platform status
- SAM failed a Swact Request due to not being In-Sync
- Swact Precheck Failed due to failure received in SIP CallP response
- Swact Precheck Failed due to failure to notify SIP CallP
- Swact Precheck Failed due to timeout waiting on SIP CallP response
- Swact PreSwact Failed due to failure received in SIP CallP response
- Swact PreSwact Failed due to failure to notify SIP CallP
- Swact PreSwact Failed due to timeout waiting on SIP CallP response
- Swact AbortSwact Failed due to failure received in SIP CallP response
- Swact AbortSwact Failed due to failure to notify SIP CallP
- Swact AbortSwact Failed due to timeout waiting on SIP CallP response
- Swact PostSwact Failed due to failure received in SIP CallP response
- Swact PostSwact Failed due to failure to notify SIP CallP
- Swact PostSwact Failed due to timeout waiting on SIP CallP response
- Disable PreCheck Failed due to failure received in SIP CallP response
- Disable PreCheck Failed due to timeout waiting on SIP CallP response
- Disable PreDisable Failed due to failure received in SIP CallP response

- Disable PreDisable Failed due to timeout waiting on SIP CallP response
- Disable AbortDisable Failed due to failure received in SIP CallP response
- Disable AbortDisable Failed due to timeout waiting on SIP CallP response
- Swact PreSwact Failed due to failure to notify SIP CallP
- Disable PreDisable Failed due to failure received from the mate SAM
- Disable PreDisable Failed due to failure to notify SIP CallP
- Disable PreDisable Failed due to timeout waiting on mate SAM response
- Disable AbortDisable Failed due to failure received from the mate SAM
- Disable AbortDisable Failed due to failure to notify SIP CallP
- Disable AbortDisable Failed due to timeout waiting on mate SAM response
- Disable Request Failed due to Callback called with existing disable request outstanding
- Disable Request Failed due to Callback called when platform not active and enabled
- Disable Inactive Failed due to Callback called when platform not in duplex
- Disable Inactive PreCheck Failed due to Callback called when SAM had a conflicting wait state
- Disable Inactive PreDisable Failed due to Callback called when SAM had a conflicting wait state
- Disable Inactive AbortDisable Failed due to Callback called when SAM had a conflicting wait state
- Disable PreCheck Failed due to failure to notify SIP CallP
- Disable PreDisable Failed due to failure to notify the Mate SAM
- Disable AbortDisable Failed due to failure to notify the Mate SAM
- Disable Active Failed due to Callback called when platform was in duplex
- Disable Active Graceful Failed due to Callback called when SIP State was not suspended
- Disable Callback called with invalid request

- SAM received a response to a Swact request that contained an invalid request
- SAM received a response to a Swact request that contained an invalid option
- SAM received a response to a Swact request that contained an invalid result
- Mate SAM failed a Prepare For COLD Swact request, reverting to a WARM swact
- Failed to notify the Mate SAM to Prepare For COLD Swact request, reverting to a WARM swact
- Timed out waiting on the Mate SAM to respond to a Prepare For COLD Swact request, reverting to a WARM swact
- SAM failed to register with DataSync

• <ErrorCode>: This is an integer code used for debugging. -1 is the default value

SIPM301

Log report SIPM301 generated when its associated critical alarm is raised because the SIP Gateway Application has transitioned to a state that indicates it should be in-service, but is actually not, while the active Session Server unit running the SIP Gateway application is in an enabled operational state. This “system busied” (SYSB) state is represented by state values as follows:

- Administrative State = Unlocked
- Operational State = Disabled
- Procedural Status = “-” or Not Terminating
- Control Status = “-” or Not Suspended

Call processing cannot occur while the SIP Gateway application is in this state.

The SIP Gateway application generates log report SIPM301 in addition to raising or clearing the alarm.

Format

The format for log report SIPM301 is as follows:

```
Apr  6 14:39:00 RTPF-SIP0 alarmd: SIPM301 CRIT TBL  SIP Gateway Maintenance
Trouble Alarm :
NCGL=RTPF-SIP0;Unit=0; SIP Gateway Application System Busy


Apr  6 14:39:01 RTPF-SIP0 alarmd: SIPM301 NONE TBL  SIP Gateway Maintenance
Trouble Alarm:
NCGL=RTPF-SIP0;Unit=0; SIP Gateway Application System Busy - Alarm Cleared
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log

Field	Value	Description
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	SIPM301	The component prefix and number of the log
Severity	Critical or None	The log severity (may be related to alarm severity)
Event Type	TBL (trouble)	The type of trouble or info recorded
Label	SIP Gateway Maintenance Trouble Alarm	Title label for the log
DeviceInfo	Alphanumeric	Info that specifies the device to which the alarm pertains
AlarmRaiseLowerText	Alphanumeric	Text indicating whether the SIP Gateway Application System Busy alarm has been raised or cleared

Action

When the SIP Gateway Application transitions out of this state (automatically or manually), this alarm is lowered. It is also lowered if the Session Server unit the application is running on leaves the enabled operational state.

When this alarm is raised, the system attempts recovery immediately. If immediate recovery is not successful, reattempts are made automatically every 30 seconds.

A manual method to attempt recovery from this alarm condition can be performed by executing the following procedures in order, found in the *Session Server Security and Administration NTP, NN10346-611*:

- Perform procedure *Lock the SIP Gateway application*
- Perform procedure *Unsuspend the SIP Gateway application*
- Perform procedure *Unlock the SIP Gateway application*

If the alarm condition persists, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SIPM302

Log SIPM302 is generated by a major alarm that is raised when the Session Server platform that the SIP Gateway Application is running on is in a duplex configuration with both units in an enabled operational state, and the SIP Gateway application state goes out of sync between the two Session Server units.

This alarm is cleared if the SIP Gateway application state becomes sync'ed between the two Session Server units and the alarm is cleared.

Format

The format for log report SIPM302 is as follows:

```
Apr 13 09:13:15 RTPF-SIP0 alarmd: SIPM302 MAJOR TBL
SIP Gateway Maintenance Sync Trouble Alarm : NCGL=RTPF-SIP0;Unit=0; SIP
Gateway Application Mtc Out Of Sync



Apr 13 09:13:45 RTPF-SIP0 alarmd: SIPM302 NONE TBL
SIP Gateway Maintenance Sync Trouble Alarm : NCGL=RTPF-SIP0;Unit=0; SIP
Gateway Application Mtc Out Of Sync - Alarm Cleared
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	SIPM302	The component prefix and number of the log
Severity	Major or None	The log severity (may be related to alarm severity)

Field	Value	Description
Event Type	TBL (trouble)	The type of trouble or info recorded
Label	SIP Gateway Maintenance Trouble Alarm	Title label for the log
DeviceInfo	Alphanumeric	Info that specifies the device to which the alarm pertains
AlarmRaiseLowerText	Alphanumeric	Text indicating whether the SIP Gateway Application Mtc Out Of Sync alarm has been raised or cleared

Action

The SIP Gateway application should attempt to sync itself automatically every 30 seconds. If there repeated sync failures, a manual method to attempt recovery from this alarm condition can be performed by executing the following procedures in order, found in the *Session Server Security and Administration NTP, NN10346-611*:

- Perform procedure *Lock the SIP Gateway application*
- Perform procedure *Suspend the SIP Gateway application*
- Perform procedure *Unsuspend the SIP Gateway application*
- Perform procedure *Unlock the SIP Gateway application*

If the alarm condition persists, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SIPM500

Log report SIPM500 is a SIP Maintenance State Change information log. The state of the SIP Application is actually updated by the callp process, but, the SIP Application maintenance message handler process thread keeps track of the last known state. When a message is received from callp, the SIP application maintenance process, running on the Session Server, checks to see if the current state matches the last known state. If it does not, then a state change log is generated. If the SIP application maintenance process updates the state, it also generates a state change log at the same time.

The SIP Gateway application generates log report SIPM500 in addition to raising the associated alarm.

State change logs include content indicated the FROM and TO states in external format, an indication of whether a user requested the change (if it was not system generated), a reason for the change, and a userid of the user that requested the change.

Format

The format for log report SIPM500 is as follows:

```
Apr 12 10:45:06 RTPF-SIP0 sipgwymtc: SIPM500 NONE INFO SIP Gateway
       Maintenance State Change
        [Administrative : Locked          -> Unlocked]
        [Operational    : Enabled         -> Enabled]
        [Control        : Not Suspended   -> Not Suspended]
        [Procedural     : Not Terminating -> Not Terminating]
        [User Requested : Yes]
        [Reason         : Unlock command issued]
        [Web User ID    : mtc]
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID or device name	Alphanumeric	The hostname or host id of the unit that generated the log

Field	Value	Description
Process Name	sipgwymtc	Identifies the NGCL or application process unit that generates the report
Log Number	SIPM500	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	SIP Maintenance State Change	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity; see section: Additional information on page 235

Action

No action is required. This is an information log only.

Associated OM registers

This log report has no associated OM registers.

Additional information

The following additional information applies to the Description field of the log entry:

- [Administrative: <AdminFrom> -> <AdminTo>]
  - Locked
  - Unlocked
  - Shutting down
- [Operational: <OperFrom> -> <OperTo>]
  - Enabled
  - Disabled
- [Control: <CtrlFrom> -> <CtrlTo>]
  - Suspended
  - Not Suspended
- [Procedural: <ProcFrom> -> <ProcTo>]
  - Terminating
  - Not Terminating
- [User Requested: <Yes|No>]
  - Yes
  - No
- [Reason: <StateChangeReason>]
  - Unsuspend command issued
  - Suspend command issued
  - Lock command issued
  - Lock command in progress
  - Lock operation complete
  - Unlock command issued
  - Shut Down command issued
  - Shut Down operation complete
  - System originated change of state
  - Timeout waiting to terminate call processing
  - Audit Failure
  - Timer Problem
  - Data corruption detected

- [Web User ID: <webuserid>]
  - If applicable, this is the web interface login ID of the user performing the maintenance that caused the state transition. If not applicable, this value is left blank. Refer to the *Overview* section of the *Session Server Security and Administration NTP, NN10346-611* for information about login IDs and user IDs and authorization categories

SIPS300

Log report SIPS300, titled T*LS dropped number of requests over time*, is generated during the alarming of dropped connection requests. This can occur either due to the connection request threshold being crossed, or due to the SIP Gateway application attempting to use TLS when TLS has not been enabled. The severity of the alarm indicates the threshold that was crossed: 10 dropped connection requests within a minute generates a minor alarm, 50 dropped requests generates a major alarm, and 100 or more dropped requests generates a critical alarm. The following message descriptions are generated:

- Dropped <number> Connections requests
- Automatically cleared due to alarm generator process death

The alarm is raised for a minimum of 30 minutes and clears on its own if the problem does not recur. Associated log SIPS600 may also be generated with this log.

Format

The format for log report SIPS300 is as follows:

```
Oct  6 20:19:53 comit.ngss.unit1 alarmd: SIPS300 MINOR TBL TLS
Dropped Connection
Request NCGL=comit.ngss.unit1;Unit=1;SIPS Dropped 10 Connections requests
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln, alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	SIPS300	The component prefix and number of the log

Field	Value	Description
Severity	None, Minor, Major, Critical	The log severity (may be related to alarm severity)
Event Type	Trouble	The type of trouble or info recorded
Label	TLS	Title label for the log
Description	see bullet list above	Detailed description of the trouble or activity

Action

Monitor incrementing (pegging) of the OM register TLS_CONNECTION_REQUESTS_DROPPED in Session Server OM group SIPGW_TLS and ensure that the event doesn't continuously recur. If it does recur, use the Session Server Configuration Management NTP, NN10338-511, to check the threshold values for the TLS connections. Consider setting the TLS connections value to a higher number, based on the number of connections expected in the given time period. If the TLS connections value is adequate, check to ensure the integrity of the central office LAN. Determine if an intruder has compromised network security. The log/alarm will be raised at least 30 minutes, and if the problem has ceased, a clear alarm log will be generated.

Associated OM registers

Refer to the Session Server Performance Management NTP, NN10342-711 for details and instructions for viewing registers in the SIPGW_TLS OM group.

Additional information

The associated log SIPS600 may also be generated with this log.

SIPS301

Log report SIPS301, titled *TLS failed certificate authentications over time*, is generated by authentication failure events. This information log indicates the reason for the authentication failures and the level of trouble. A critical alarm indicates a very serious problem while a minor alarm can indicate transient failures or the beginning of a series of authentication failures.

The following message descriptions are generated:

- Failed <number> certificate authentications:
  which indicates the number of times this event occurred in the last minute before the alarm was raised.
- Automatically cleared due to alarm generator process death

Format

The format for log report SIPS301 is as follows:

```
Feb 9 13:03:50 comit.ngss.unit1 alarmd: SIPS301 CRIT TBL TLS Failed Authentication
NCGL=comit.ngss.unit1;Unit=0;SIPS Failed 28 certificate authentications

Feb 9 13:08:10 comit.ngss.unit1 alarmd: SIPS301 NONE TBL TLS Failed Authentication
NCGL=comit.ngss.unit1;Unit=0;SIPS Automatically cleared due to alarm
generator process death
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	SIPS301	The component prefix and number of the log

Field	Value	Description
Severity	None, Minor, Major, or Critical	The log severity (may be related to alarm severity)
Event Type	Info, Trouble	The type of trouble or info recorded
Label	TLS	Title label for the log
Description	see the bullet list above	Detailed description of the trouble or activity

Action

On a major or critical severity log, check to ensure that the security certificate and key provided to the SIP Gateway application are in the correct directory (as pointed to by the database entry). Then ensure that the certificate and key files are not corrupted or altered. Use the Certificate Management Tool to ensure that the certificate and key files are meant to be used together. Contact your next level of support or Nortel GNPS for support with these activities.

Associated OM registers

Monitor incrementation of the OM registers TLS_CONNECTION_REQUESTS_FAILED and TLS_HANDSHAKE_AUTHENTICATION_FAILED in Session Server OM group SIPGW_TLS. Refer to the Session Server Performance Management NTP, NN10342-711 for details and instructions on viewing registers in the SIPGW_TLS OM group.

Additional information

This log report has no additional information.

SIPS302

Log report SIPS302, titled TLS Local certificate is expiring soon, is generated as a result of regular alarm process checks to ensure the local server certificate continues to be valid. The expiration date contained in the certificate is checked on a daily basis. As the expiration date of the certificate approaches, an alarm is raised and log generated within 31 days (minor alarm), 15 days (major alarm), or 5 days (critical alarm) of the expiration date. For certificates that have already expired, a critical alarm and log are generated, and authentication failures (log SIPS601) will be generated for any connections that are attempted.

Format

The format for log report SIPS302 is as follows:

```
Oct 8 13:14:17 comit.ngss.unit0 alarmd: SIPS302 MINOR TBL TLS
Local Certificate is Expiring Soon
NCGL=comit.ngss.unit0;Unit=0;SIPS TLS Local Certificate is Expiring Soon
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	SIPS302	The component prefix and number of the log
Severity	None, Minor, Major, or Critical	The log severity (may be related to alarm severity)
Event Type	Info, Trouble	The type of trouble or info recorded

Field	Value	Description
Label	TLS	Title label for the log
Description	Local Certificate is Expiring Soon	Detailed description of the trouble or activity

Action

Use the Certificate Management Tool to create a new self-signed certificate (if using self-signed certificates) or to generate a certificate signing request (for creating CA-signed certificates). Refer to the Session Server Security and Administration NTP, NN10346-611, for procedures on creating new CA-signed or self-signed security certificates. Add the new certificate to the system using procedures in the Session Server Configuration Management NTP, NN10338-511.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

SIPS305

Log report SIPS305, titled *TLS initialization logs*, is generated during the initialization (unlock) of the SIP Gateway application. It indicates that there is a problem with the initialization of the application. The following message descriptions may be generated:

- TLS Local Key and Certificate do not match
- TLS Failed client init
- TLS Failed Server init
- TLS Failed to load Certificate
- TLS Failed to load Key
- TLS Failed to Init
- TLS Failed to get pointer
- TLS Failed to create thread
- TLS Failed Local Certificate Policy
- TLS is Not Enabled — logs with this reason also indicate the device name and unit number

Format

The format for log report SIPS305 is as follows:

```
Feb 9 13:11:39 comit.ngss.unit1 sipgwyappln: SIPS305 CRIT INIT TLS
TLS Failed to load Key

Mar 1 10:06:53 comit.ngss.unit0 alarmd: SIPS305 CRIT TBL TLS is Not Emabled
NCGL=comit.ngss.unit0;Unit=1;SIPS TLS is Not Enabled
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln	Identifies the NGCL or application process unit that generates the report

Field	Value	Description
Log Number	SIPS305	The component prefix and number of the log
Severity	Critical	The log severity (may be related to alarm severity)
Event Type	Initialization	The type of trouble or info recorded
Label	TLS	Title label for the log
Description	see details above for the description	Detailed description of the trouble or activity

Action

Perform the following activities in the order listed:

1. Check to ensure that the certificate and key files provided to the SIP Gateway application are in the correct directory (as pointed to by the database entry). This location is typically `/opt/base/shared/ssl`.
2. Ensure that the certificate and key files themselves are not corrupted or altered.
3. Ensure that the certificate and key files are meant to be together (by running the **cert_mgnt** tool). If necessary, contact your next level of support or Nortel GNPS for assistance with this activity.
4. Once the problem is resolved, and the SIP Gateway application is initialized (unlocked) again, there will be 3 logs indicating problem resolution: SIPM500, SIPS605, SIPS604.

Associated OM registers

This log report has no associated OM registers.

Additional information

Normally, the Certificate Management Tool will provision the certificate and key files properly. If this tool has not been used to successfully set up security certificates prior to attempting to bring the SIP Gateway application into service, unexpected results could occur. Extra information as to the cause of the problem will likely reside in the SIP Gateway application initialization trace logs provided in the /opt/apps/logs directory. Look for entries labeled: siptrace.<date>.server.<pid>.

SIPS600

Log report SIPS600, titled *TLS connection request dropped*, is generated during the connection setup of SIP Gateway application callp processes. This is an information log only and is not associated with an alarm. The following message descriptions are generated:

- Dropped TLS Handshake request, monitor OMs
- Dropped TLS Handshake request, TLS is not enabled

Format

The format for log report SIPS600 is as follows:

```
Oct 8 15:17:07 comit.ngss.unit1 sipgwyappln: SIPS600 MINOR INFO TLS
Dropped TLS Handshake request, monitor OMs
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPS600	The component prefix and number of the log
Severity	Minor	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	TLS	Title label for the log
Description	see bullet list above	Detailed description of the trouble or activity

Action

If the message “Dropped TLS Handshake request, monitor OMs” is displayed only once or twice, there is likely a transient connection problem. Monitor incrementing of the OM register TLS_CONNECTION_REQUESTS_DROPPED in Session Server OM group SIPGW_TLS and ensure that the event doesn’t continuously recur. If it does recur, use the Session Server Configuration NTP, NN10338-511, to check the threshold values for the TLS connections. Consider setting the TLS connections value to a higher number, based on the number of connections expected in the given time period. If the TLS connections value is adequate, check to ensure the integrity of the central office LAN. Determine if an intruder has compromised network security.

If the message “TLS is not enabled” is displayed, refer to other available logs and ensure that the SIP Gateway application initialized properly.

Associated OM registers

Refer to the Session Server Performance Management NTP, NN10342-711 for details and instructions for viewing registers in the SIPGW_TLS OM group.

Additional information

This log report has no additional information.

SIPS601

Log report SIPS601, titled *TLS authentication failure <reason>*, is generated from TLS authentication failure events. This information log indicates the reason for the authentication failures. Refer to the Additional information section for log message details.

Format

The format for log report SIPS601 is as follows:

```
Oct 8 16:36:56 comit.ngss.unit1 sipgwyappln: SIPS601 MINOR INFO TLS
common name: 47.129.118.195, reason: certificate has expired
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPS601	The component prefix and number of the log
Severity	Minor	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	TLS	Title label for the log

Field	Value	Description
Common Name	The common name in the security certificate that the remote SIP server uses.	The common name in the X.509 security certificate that the remote SIP server is presenting to the Session Server.
Description	Refer to Additional information	Detailed description of the trouble or activity

Action

This information log report requires no action; however, an excessive amount of authentication failures may have associated alarms. Check for additional alarms or associated OMs.

Associated OM registers

Monitor incrementation of the OM registers TLS_CONNECTION_REQUESTS_FAILED and TLS_HANDSHAKE_AUTHENTICATION_FAILED in Session Server OM group SIPGW_TLS. Refer to the Session Server Performance Management NTP, NN10342-711 for details and instructions for viewing registers in the SIPGW_TLS OM group.

Additional information

One or more of the following detailed reasons may be part of the information log:

- unable to get issuer certificate
- unable to get certificate CRL
- unable to decrypt certificate's signature
- unable to decrypt CRL's signature
- unable to decode issuer public key
- certificate signature failure
- CRL signature failure
- certificate is not yet valid
- CRL is not yet valid
- certificate has expired
- CRL has expired

- format error in certificate's notBefore field
- format error in certificate's notAfter field
- format error in CRL's lastUpdate field
- format error in CRL's nextUpdate field
- out of memory
- self signed certificate
- self signed certificate in certificate chain
- unable to get local issuer certificate
- unable to verify the first certificate
- certificate chain too long
- certificate revoked
- invalid CA certificate
- path length constraint exceeded
- unsupported certificate purpose
- certificate not trusted
- certificate rejected
- application verification failure
- subject issuer mismatch
- authority and subject key identifier mismatch
- authority and issuer serial number mismatch
- key usage does not include certificate signing
- unable to get CRL issuer certificate
- unhandled critical extension
- key usage does not include CRL signing
- unhandled critical CRL extension

SIPS604

Log report SIPS604, titled *TLS initialization logs*, is generated during initialization (unlock) of the SIP Gateway application, indicating when the current local certificate effective date and when it will expire, using the format Year=<YYYY>, Month = <MM>, Day = <DD>. This is an information log only and is not directly associated with an alarm.

Format

The format for log report SIPS604 is as follows:

```
Oct 8 15:17:07 comit.ngss.unit1 sipgwyappln: SIPS604 NONE INFO TLS
Local Certificate Effective: Year=2004, Month = 10, Day = 8

Oct 8 15:17:07 comit.ngss.unit1 sipgwyappln: SIPS604 NONE INFO TLS
Local Certificate Expires: Year=2005, Month = 10, Day = 8
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPS604	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	TLS	Title label for the log
Description	see details above for the description	Detailed description of the trouble or activity

Action

No action is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

No additional information is currently available.

SIPS605

Log report SIPS605,titled *TLS initialization logs*, is generated during initialization (unlock) of the SIP Gateway application, indicating that TLS Security is enabled. This is an information log only and is not directly associated with an alarm. A SIPS604 log may be generated with this log.

Format

The format for log report SIPS605 is as follows:

```
Oct 8 15:17:07 comit.ngss.unit1 sipgwyappln: SIPS605 NONE INFO TLS
TLS Security Enabled
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPS605	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	TLS	Title label for the log
Description	see details above for the description	Detailed description of the trouble or activity

Action

No action is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

No additional information is currently available.

SIPS606

Log report SIPS606, titled *TLS attempt to add trusted certificate failed*, is generated when there is a problem importing the trusted certificate provisioned into the database using the CS 2000 Session Server Manager GUI. This is an information log only and is not associated with an alarm. The following message descriptions are generated:

- Failed to add Trusted CA name server
- Failed to add Trusted CA name <name>

Format

The format for log report SIPS606 is as follows:

```
Oct 8 13:41:47 comit.ngss.unit1 sipgwyappln: SIPS606 NONE INFO TLS
Failed to add Trusted CA name servername
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPS606	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	TLS	Title label for the log
Description	see bullet list above	Detailed description of the trouble or activity

Action

The security certificate being used is not correct or has become corrupted, and is unable to be loaded by the SIP Gateway application. Try to reprovision the certificate (using a different name) or delete the certificate, then re-add it. Refer to the Session Server Configuration Management NTP, NN10338-511, for procedures on provisioning existing security certificates. Refer to the Session Server Security and Administration NTP, NN10346-611, for procedures on creating new CA-signed or self-signed security certificates.

Associated OM registers

This log report has no associated OM registers.

Additional information

If log SIPS606 is generated along with authentication log SIPS301, it is likely due to the failure to properly provision the trusted certificate for the remote server. Retrieve the remote server's public self-signed certificate and add it to the database using procedures from the Session Server Configuration Management NTP, NN10338-511.

SIPS607

Log report SIPS607, titled *TLS Connection Request Failed*, is generated to provide details into which remote server is not able to connect with the local server (SIP Gateway application running on the Session Server). This log supplements log SIPS601 and is an information log only and is not directly associated with an alarm.

Format

The format for log report SIPS607 is as follows:

```
Feb 16 09:53:44 comit.ngss.unit1 sipgwyappln: SIPS607 NONE INFO TLS
Connection Request Failed: Server: AURUM, IP Address: 47.129.118.195
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPS607	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	TLS	Title label for the log
Description	Connection Request Failed	Detailed description of the trouble or activity

Field	Value	Description
Server:	Refer to the Additional information section	Name of the remote SIP server as it is provisioned in the Session Server database. This value corresponds to the name of the remote SIP server.
IP Address	IP address of the remote server unable to connect with the Session Server	The IP address of the remote SIP server.

Action

This information log report requires no action; however, if there are an excessive number of SIPS607 logs, check for additional alarms, related SIPS601 logs and associated OMs.

Associated OM registers

Monitor incrementation the OM registers TLS_CONNECTION_REQUESTS_FAILED in Session Server OM group SIPGW_TLS. Refer to the Session Server Performance Management NTP, NN10342-711 for details and instructions for viewing registers in the SIPGW_TLS OM group.

Additional information

If the value of the server name is NULL, this log, together with the SIPS601 log, indicates that the remote SIP server is not provisioned in the Session Server database

If the value of the server name is not NULL, the SIPS607 log, together with the SIPS601 log, indicates which remote server is not able to connect with the Session Server, and the reason why the remote server is not able to connect. Verify provisioning of the security certificates on the remote SIP server and on the local Session Server.

STGW700

Log report STGW700 is an information log that is generated by the SIP Gateway application.

This log may be generated when call processing activity is interrupted or negatively impacted, such as during an upgrade.

Format

The format for log report STGW700 is as follows:

```
May 11 15:09:33 PGk-1 sipgwyappln: STGW700 NONE INFO SIPCALLP
supportedExtensionList was Null defaulted to 100rel

Aug 17 12:11:33 rtpg-duplex-unit-1 sipgwyappln: STGW700 NONE INFO SIPCALLP
No Active Server for SIP Link 5

Sep 13 15:50:59 cablab.ss.unit0 sipgwyappln: STGW700 NONE INFO LINKMTC
mgcHostName in Config Data is null

Sep 13 15:56:49 cablab.ss.unit0 sipgwyappln: STGW700 NONE INFO SIPCALLP
No Active Server for SIP Link 2

Sep 17 09:42:00 OTT2.SS0 sipgwyappln: STGW700 NONE INFO SIPCALLP
new message received with bad syntax. OTT2NGSS

Sep 17 09:42:25 OTT2.SS0 sipgwyappln: STGW700 NONE INFO SIPCALLP
new message received with bad syntax. CABLABNGSS

May  9 13:45:26 rtpfngss1 alarmd: STGW700 CRIT TBL  SIPOVLD
NCGL=rtpfngss1;Unit=1;SIPC CPU occupancy critical alarm

May  9 13:45:26 rtpfngss1 sipgwyappln: STGW700 NONE INFO SIPOVLD
FCR Change OLD FCR: 100 NEW FCR: 90

May 12 10:29:00 rtpfngss1 sipgwyappln: STGW700 NONE INFO SIPOVLD
All babbling node IPs re-enabled due to initialization
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln or alarmd	Identifies the subsystem that generates the report
Log Number	STGW700	The component prefix and number of the log
Severity	NONE, CRIT, MAJOR	The log severity (may be related to alarm severity)
Event Type	INFO	The type of trouble or info recorded
Label	SIPCALLP, LINKMTC, SIPOVLD	Title label for the log
Description	LogMessage	Detailed description of the messages, refer to section Additional information.

Action

No action is required. If this log persists, contact your next level of support.

Associated OM registers

For log reports with a label of SIPCALLP, OM group SIPGW_CALLP is related. For log reports with a label of SIPOVLD, OM group SIPGW_OVERLOAD is related.

Additional information

The following additional information applies to the Log Message field of the log entry:

- Failed to send SUBSCRIBE for detecting Fax Modem Tones
- AUDIT CALL FORCE RELEASE CALLID : 0022.4960-14-10-04-39.73@RALEIGH GWC 172.17.40.44 GCP State : 9

- LINKMTC mgcHostName in Config Data is null
- PostGainNotifyCallp Called on INACTIVE side
- Sync call to the standby unit failed with callid callId
- GCP NewCall received for Unsupported Agent: agentType
- No more CallDataBlocks to process CallID: callId
- Failed to add ISUP payload for call callId
- Remote SIP server not mapped for SIP LINK Index SipLinkIdx
- No Active Server for SIP Link SipLinkIdx
- HandleNewCall::Failed to Set MDB for callid callId
- No GCP Nodes to process call with callid callId
- Unauthorized Call attempt from MGC DestMgc
- HandleSipUPDATERequest::MDB Parsing for UPDATE failed for callid callId
- HandleACK::MDB Parsing for ACK failed for callid callId
- Handle200OKINVITERecvd::MDB Parsing for 200 OK INVITE failed for callid callId
- Incompatible media format received in 200 OK response to INVITE.
- Handle200OKINVITERecvd::Failed to send ACK for callid callId
- Handle200OKINVITERecvd::Failed to get Outbound Message for callid callId
- Handle200OKINVITERecvd::Failed to add 305 warning header for callid callId
- HandleReINVITE::MDB Parsing for Re INVITE failed for callid callId
- HandleSipINFORequest::MDB Parsing for INFO failed for callid callId
- HandleACKReINVITE::MDB Parsing for ACK failed for callid callId
- new message received with bad syntax start-line. msgDestName
- new message received with bad syntax. msgDestName
- Unable to Get Received Message (ACK) for callid callId
- Module:Procedure Null App Call Context
- Module:Procedure Unable to Get Received Message
- Media Error: CALLID: callId - 488 Not Acceptable Here Received
- Media Error: CALLID: callId - 606 Not Acceptable Received
- Incompatible media format, call rejected.

- Media type not available, call rejected.
- GCP Socket Open Failed
- Failed to get Active IP Address
- Bind for GCP Socket Failed
- supportedExtensionList was Null defaulted to 100rel
- NGSS Profile Data Creation Failed for Server sipServerName

XTS300

Log report XTS300 indicates that system random access memory (RAM) resources are low.

The NCGL operating system generates a log report whenever a minor, major or critical XTS300 OutofMemory alarm is raised or if the existing alarm is escalated. This is a quality of service alarm indicating that memory resources are low or near exhaustion. Memory resource limitation could impact the quality of service of the Session Server or Policy Controller, leading to partial loss of service.

Format

The format for log report XTS300 is as follows:

```
APR17 07:46:06 ngss-1 XTS300 minor FLT Memory
Unit Number : 0, ACTIVE
Available memory is between 125MB and 150MB;
              minor threshold reached.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	N/A	Identifies the NGCL or application process unit that generates the report
Log Number	XTS300	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded

Field	Value	Description
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. Refer to *Session Server Fault Management*, NN10332-911 for a description of how to monitor the connectivity and network status for both Session Server units. Refer to *Policy Controller Fault Management,* NN10438-911 for a description of how to monitor the connectivity and network status for both Policy Controller units.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS301

Log report XTS301 indicates that the CPU load average for one or more time segments has exceeded a preset threshold.

The Session Server or Policy Controller platform generates log report XTS301 in addition to the alarm.

Format

The format for log report XTS301 is as follows:

```
APR17 07:46:06 ngss-1 XTS301 minor FLT CPU Load
Unit Number : 0, ACTIVE
1 minute load average is between 10.00 and 20.
00; minor threshold reached.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	N/A	Identifies the NGCL or application process unit that generates the report
Log Number	XTS301	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (Fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. Refer to *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the status of CPU and memory related resources for the active unit.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS302

Log report XTS302 indicates that free space on the root file system is low.

The Session Server or Policy Controller platform generates log report XTS302 in addition to the alarm.

Format

The format for log report XTS302 is as follows:

```
APR17 07:47:46 ngss-1 XTS302 minor FLT Disk/Storage
Unit Number : 0, ACTIVE
Percentage of root free disk space is less than
or equal to 5.00; critical threshold reached.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	N/A	Identifies the NGCL or application process unit that generates the report
Log Number	XTS302	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble

Action

This alarm may clear on its own. Refer to *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the status of disk drive resources for the active unit.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS303

Log report XTS303 indicates that at least one software process has terminated abnormally and may retain system resources such as memory space or CPU usage (zombie process).

The Session Server or Policy Controller platform generates log report XTS303 in addition to the alarm.

Format

The format for log report XTS303 is as follows:

```
APR17 08:06:23 ngss-1 XTS303 minor FLT  Zombie Process
Unit Number : 0, ACTIVE
Number of zombie processes is between 5 and 10;
              minor threshold reached.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	N/A	Identifies the NGCL or application process unit that generates the report
Log Number	XTS303	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. Refer to *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the status of zombie processes for the active unit.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS304

Log report XTS304 indicates one or more of the Network File System (NFS) mounted file systems is inaccessible. Each unit mounts a file system from the mate unit. This log report is expected during upgrades or any time the mate unit is unavailable.

The unit generates log report XTS604 when the alarm clears.

Format

The format for log report XTS304 is as follows:

```
May  6 17:25:30 ngss-1 alarmd: XTS304 MINOR FLT  NFS Mount
Not Accessible NCGL=ngss-1;Unit=0 Number of accessible
NFS mounts is equal to 0; minor threshold reached
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS304	The component prefix and number of the log
Severity	minor	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm is raised in addition to more severe alarms such as Mate is unavailable and point to point (PTP) failure. If connectivity to the mate is lost or if the mate unit is offline, then this alarm clears when communication with the mate is restored.

If the mate unit is available, clear connectivity related alarms. Connectivity to the mate over the PTP link, physically provided by the crossover cables, is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

XTS305

Log report XTS305 indicates that the platform software lost time synchronization to one or more Network Time Protocol (NTP) servers, or the drift is excessive.

The Session Server or Policy Controller platform generates log report XTS305 in addition to the alarm.

Format

The format for log report XTS305 is as follows:

```
Feb 13 10:42:05 rtpsngss1unit1 alarmd: XTS305 MAJOR FLT
NTP Error NCGL=rtpsngss1unit1;Unit=1 Host is not communicating
with any NTP server(s);
No. of configured server(s): 1; No. of accessible server(s): 0.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS305	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	NTP Error	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own; however, if the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS306

Log report XTS306 indicates that CPU utilization has exceeded a preset threshold.

The Session Server or Policy Controller platform generates log report XTS306 in addition to the alarm.

Format

The format for log report XTS306 is as follows:

```
May 25 10:13:05 yin alarmd: XTS306 MINOR FLT CPU Utilization NCGL=yin;
Unit=0 5 minute percent idle cpu utilization is below 5.00,
minor threshold reached.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS306	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. Refer to *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the status of CPU and memory related resources for the active unit.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS309

Log report XTS309 indicates that a peripheral hardware component (such as an ethernet card) has a Peripheral Component Interconnect (PCI) bus fault, Error Checking and Correction (ECC) memory fault, or a parity error.

The Session Server or Policy Controller platform generates log report XTS309 in addition to the alarm.

Format

The format for log report XTS309 is as follows:

```
AUG6 08:13:22 ngss-1 XTS309 critical FLT  Hardware Fault
Unit Number : 1, INACTIVE
Data parity critical threshold is reached;
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	Alphanumeric	Identifies the NGCL or application process unit that generates the report
Log Number	XTS309	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. If the alarm persists, refer to procedure *Reboot a Session Server unit* in the Session Server Security and Administration NTP, NN10346-611 or *Reboot a Policy Controller unit* in the Policy Controller Security and Administration NTP, NN10434-611, for a description how to reboot the affected unit. After the reboot, check the resulting system status in *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911.

If the alarm persists, consider replacing the unit.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS315

Log report XTS315 is generated when the inactive unit becomes disabled and is not available.

The Session Server or Policy Controller platform generates log report XTS315 in addition to the alarm.

Format

The format for log report XTS315 is as follows:

```
Sep 13 15:00:24 cablab.ss.unit1 alarmd: XTS315 MAJOR FLT  Simplex Node
NCGL=cablab.ss.unit1;Unit=1 The state is Standby Disabled.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	Alphanumeric	Identifies the NGCL or application process unit that generates the report
Log Number	XTS315	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. Refer to *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the status of the application on both units.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS331

Log report XTS331 indicates that the Session Server or Policy Controller active unit cannot communicate to the mate unit through the ethernet connections.

The Session Server or Policy Controller platform generates log report XTS331 in addition to the alarm.

Format

The format for log report XTS331 is as follows:

```
Oct 25 09:53:18 cablab.ss.unit1 alarmd: XTS331 MAJOR FLT
Mate Connectivity NCGL=cablab.ss.unit1;Unit=1 Link0:
INSV, mateCon: UNAVAIL, netCon: AVAIL; Link1: INSV,
mateCon: UNAVAIL, netCon: AVAIL;  PTPLink: INSV, mateCon: UNAVAIL;
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	Alphanumeric	Identifies the NGCL or application process unit that generates the report
Log Number	XTS331	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. Refer to *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the connectivity and network status for both units.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS335

Log report XTS335 is generated in response to a Communications Subsystem Failure alarm when one or both PTP links is down.

The Session Server or Policy Controller platform generates log report XTS335 in addition to the alarm.

Format

The format for log report XTS335 is as follows:

```
Jul 22 09:43:04 cablab alarmd: XTS335 MAJOR FLT Link Connectivity ss.unit1;
Unit=1 Link0:INSV, mateCon: AVAIL, netCon: AVAIL;Link1:INSV, mateCon: AVAIL,
netCon: AVAIL; PTPLink: PTP0-SYSB, mateCon: AVAIL;


Jul 22 10:32:33 cablab alarmd: XTS335 MAJOR FLT Link Connectivity ss.unit1;
Unit=1 Link0: INSV, mateCon: AVAIL, netCon: AVAIL; Link1:INSV, mateCon: AVAIL,
netCon: AVAIL; PTPLink: BOTH_SYSB, mateCon: AVAIL;
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	Alphanumeric	Identifies the NGCL or application process unit that generates the report
Log Number	XTS335	The component prefix and log number
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded

Field	Value	Description
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. Refer to *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the connectivity and network status for both units.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS336

Log report XTS336 indicates that one or more ethernet links are unable to communicate with the network.

The Session Server or Policy Controller platform generates log report XTS336 in addition to the alarm.

Format

The format for log report XTS336 is as follows:

```
Sep 21 09:17:26 cablab.ss.unit1 alarmd: XTS336 MAJOR FLT Network
Connectivity NCGL=cablab.ss.unit1;Unit=1 Link0: INSV, mateCon: AVAIL,
netCon: UNAVAIL; Link1: INSV, mateCon: AVAIL, netCon: AVAIL; PTPLink:
INSV, mateCon: AVAIL;
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	Alphanumeric	Identifies the NGCL or application process unit that generates the report
Log Number	XTS336	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. Refer to *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the connectivity and network status for both units.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS351

Log report XTS351 indicates a response to several CON and APL alarms because the mate Session Server or Policy Controller unit is unavailable or status information for the mate unit is unavailable at the maintenance interface.

The Session Server or Policy Controller platform generates log report XTS351 in addition to the alarm.

Format

The format for log report XTS351 is as follows:

```
Sep 21 09:27:14 cablab.ss.unit0 alarmd: XTS351 MAJOR FLT No Mate
Communication (simplex) NCGL=cablab.ss.unit0;Unit=0 Mate unit is
unavailable.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	Alphanumeric	Identifies the NGCL or application process unit that generates the report
Log Number	XTS351	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. Refer to *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the connectivity status for the active and standby units.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS355

Log report XTS355 indicates the inactive unit is jammed to prevent a Switch of Activity (SwAct).

The Session Server or Policy Controller platform generates log report XTS355 in addition to the alarm.

Format

The format for log report XTS355 is as follows:

```
Sep 20 12:46:23 cablab.ss.unit0 alarmd: XTS355 MINOR FLT  Jam Inactive Unit
NCGL=cablab.ss.unit0;Unit=0 Inactive JAMMED
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	Alphanumeric	Identifies the NGCL or application process unit that generates the report
Log Number	XTS355	The component prefix and number of the log
Severity	minor	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. Refer to *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the status of CPU and memory related resources for the active unit.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS391

Log report XTS391 indicates that a disk drive:

- has failed (major) or has been removed from the system chassis (critical)
- has been removed from the NCGL for maintenance or upgrade but is still installed in the chassis (major)
- is having its filesystem rebuilt and its performance is degraded (minor)

The Session Server or Policy Controller platform generates log report XTS391 in addition to the alarm. When the alarm condition is cleared, a log XTS691 is generated.

Format

The format for log report XTS391 is as follows:

```
Sep 20 15:37:47 cablab.ss.unit1 alarmd: XTS391 MAJOR UNEQ Disk Missing
NCGL=cablab.ss.unit1;Unit=1; Array:
'/dev/md1
' (ntvg) Status: A physical
disk has been removed from the array.

Sep 20 15:38:22 cablab.ss.unit1 alarmd: XTS391 MINOR INIT Array Rebuilding
NCGL=cablab.ss.unit1;Unit=1; Array:
'/dev/md0
' (/boot) Status: The array
is currently being rebuilt.

Sep 20 15:38:22 cablab.ss.unit1 alarmd: XTS391 MINOR INIT Array Rebuilding
NCGL=cablab.ss.unit1;Unit=1; Array:
'/dev/md1
' (ntvg) Status: The array is
currently being rebuilt.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	Alphanumeric	Identifies the NGCL or application process unit that generates the report
Log Number	XTS391	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

Determine the cause of the alarm and refer to *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the status of Disk Storage resources for the affected unit.

Replace the failed disk drive. Refer to the procedure in *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS392

Log report XTS392 indicates a error result has been returned from regularly occurring NGCL audit testing for any of the following conditions:

- Magneto Hardware Chassis Fault (equipment malfunction or failure)
- Self Test Unavailable (NCGL malfunction or process failure)
- Self Test Hardware Error (equipment malfunction or failure)
- Self Test Query Error (equipment malfunction or failure)
- Self Test Corrupted Error (equipment malfunction or failure)
- Self Test Device Failure (equipment malfunction or failure)

The severity level of the alarm is determined by the conditions listed above.

The Session Server or Policy Controller platform generates log report XTS392 in addition to the alarm. When the alarm condition is cleared, a log XTS692 is generated.

Format

The format for log report XTS392 is as follows:

```
May 19 10:31:33 loopback alarmd: XTS392 MAJOR FLT  Self Test
NCGL=localhost; Unable to communicate with BMC to get results. cc=0

May 19 11:40:44 unit0 alarmd: XTS392 MAJOR FLT  Self Test NCGL=unit0;
Unable to communicate with BMC to get results. cc=0

May 19 12:36:27 yin alarmd: XTS392 MAJOR FAIL Chassis Fault NCGL=yin;Unit=0;
Power overload detected.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log

Field	Value	Description
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS392	The component prefix and number of the log
Severity	minor, major	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This log report requires no action. If the alarm persists, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS395

Log report XTS395 indicates a error result has been returned from regularly occurring NCGL file system audit tests:

- Self Test Device Filesystem Threshold Exceeded; this is a quality of service alarm indicating that memory resources are low
- Filesystem Test Failure (minor) due to low disk space
- Filesystem Test Failure (critical) due to test failure

The Session Server or Policy Controller platform generates log report XTS395 in addition to the alarm. When the alarm condition is cleared, a log XTS695 is generated.

Format

The format for log report XTS395 is as follows:

```
May  4 13:02:58 fred alarmd: XTS395 MINOR FLT
Filesystem Error NCGL=fred;Unit=0 Status: Alarm raised.
Filesystem is < /boot >. Test results: Stat(Success) CreateDir(Success)
CreateFile(Success) WriteFile(No space left on device) ReadFile(Success)
RemoveFile(Success) RemoveDir(Success)
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS395	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded

Field	Value	Description
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This log report requires no action. If the alarm persists, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS600

Log report XTS600 is written by the NCGL operating system when the conditions which raised alarm XTS300 have been cleared.

Format

The format for log report XTS600 is as follows:

```
Apr 7 14:11:45 sp2k-1 logman: XTS600 NONE INFO Memory Alarm Cleared
Unit Number : 0, UNDETERMINED
Description : Available memory is greater than the minor threshold
value of 150MB
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS600	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Memory Alarm Cleared	Title label for the log
Description	Refer to originating XTS300 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS601

Log report XTS601 is written by the NCGL operating system when the conditions which raised alarm XTS301 have been cleared.

Format

The format for log report XTS601 is as follows:

```
Apr 7 14:11:45 sp2k-1 logman: XTS601 NONE INFO CPU Alarm
Cleared Unit Number : 0, UNDETERMINED
Description : 1 minute load average is less than 10.00; no threshold reached
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS601	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	CPU Alarm	Title label for the log
Description	Refer to originating XTS301 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS602

Log report XTS602 is written by the NCGL operating system when the conditions which raised alarm XTS302 have been cleared.

Format

The format for log report XTS602 is as follows:

```
Apr 29 14:11:39 yang logman: XTS602 NONE INFO Disk Alarm Cleared
Unit Number : 1, ACTIVE
Description : Percentage of root free disk space is greater than 15.00.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS602	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Memory Alarm Cleared	Title label for the log
Description	Refer to originating XTS302 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS603

Log report XTS603 is written by the NCGL operating system when the conditions which raised alarm XTS303 have been cleared.

Format

The format for log report XTS603 is as follows:

```
Apr 7 14:11:46 sp2k-1 logman: XTS603 NONE INFO Zombie Process Alarm Cleared
Unit Number : 0, UNDETERMINED
Description : Number of zombie processes is less than 5.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS603	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Memory Alarm Cleared	Title label for the log
Description	Refer to originating XTS303 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS604

Log report XTS604 is written by the NCGL operating system when the conditions which raised alarm XTS304 have been cleared.

Format

The format for log report XTS604 is as follows:

```
May  6 18:50:22 ngss-1 logman: XTS604 NONE INFO NFS Mounts Accessible
Unit Number : 0, ACTIVE         Description : Number of accessible
NFS mounts is greater than 0.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS604	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	NFS Mounts Accessible	Title label for the log
Description	Refer to originating XTS304 alarm for details	Detailed description of the trouble or activity

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS605

Log report XTS605 is written by the NCGL operating system when the conditions which raised alarm XTS305 have been cleared.

Format

The format for log report XTS605 is as follows:

```
Sep 13 15:04:20 cablab.ss.unit1 alarmd: XTS605 NONE INFO NTP
Error NCGL=cablab.ss.unit1;Unit=1 Host is not communicating with any NTP
server(s); No. of configured server(s): 3; No. of accessible server(s): 0.

Sep 13 15:04:40 cablab.ss.unit1 alarmd: XTS605 NONE INFO NTP
Error NCGL=cablab.ss.unit1;Unit=1 Host is not synchronized to any NTP
server(s); No. of configured server(s): 3; No. of accessible server(s): 3.

Sep 13 15:07:50 cablab.ss.unit1 alarmd: XTS605 NONE INFO NTP
Error NCGL=cablab.ss.unit1;Unit=1 Host lost synchronization to one or more
NTP servers; No. of configured server(s): 3; No. of accessible server(s):
3; Host synchronized to: 2 server(s).

Sep 13 15:20:22 cablab.ss.unit1 alarmd: XTS605 NONE INFO NTP
Error NCGL=cablab.ss.unit1;Unit=1 Time offset is greater than the defined
threshold; Offset from NTP server 10.65.96.13: 61ms; Threshold: (+/-)50ms.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS605	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded

Field	Value	Description
Label	NTP Alarm Cleared or NTP Error	Title label for the log
Description	Refer to originating XTS305 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS606

Log report XTS606 is written by the NCGL operating system when the conditions which raised alarm XTS306 have been cleared.

Format

The format for log report XTS606 is as follows:

```
Apr 29 14:11:39 yang logman: XTS606 NONE INFO CPU Utilization Cleared
Unit Number : 1, ACTIVE
Description : 5 minute percent idle cpu utilization is above 5.00,
no threshold reached.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS606	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	CPU Utilization Cleared	Title label for the log
Description	Refer to originating XTS306 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS609

Log report XTS609 is written by the NCGL operating system when the conditions which raised alarm XTS309 have been cleared.

Format

The format for log report XTS609 is as follows:

```
Nov 4 11:00:58 OTT2.SS0 logman: XTS609 NONE INFO
Hardware Fault Cleared Unit Number : 0, ACTIVE Description :
HWMON Fault Inserted through debug tool
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS609	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Hardware Fault Cleared	Title label for the log
Description	Refer to originating XTS309 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS615

Log report XTS615 is written by the NCGL operating system when the conditions which raised alarm XTS315 have been cleared.

Note: When a SwAct occurs, the SIP Gateway application database loses synchronization. An alarm and SIPM302 log are generated, indicating loss of synchronization. After the SwAct has completed, the SIP Gateway application database returns to a synchronized state, and a follow-up SIPM-302 log is generated, indicating that the alarm has cleared.

Format

The format for log report XTS615 is as follows:

```
Apr 7 09:17:04 sp2k-1 alarmd: XTS615 NONE INFO Duplex Node NCGL=sp2k-1;
Unit=0 State has changed from Standby Disabled to Standby Enabled.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS615	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Duplex Node	Title label for the log
Description	Refer to the originating XTS315 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS616

Log report XTS616 is written by the NCGL operating system when the conditions which raised alarm XTS316 have been cleared.

Format

The format for log report XTS616 is as follows:

```
Apr 7 09:37:32 sp2k-1 logman: XTS616 NONE INFO Application In-Service
Unit Number : 0, UNDETERMINED
Description : The state is Running.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS616	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Application In-service	Title label for the log
Description	Refer to originating XTS316 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS631

Log report XTS631 is written by the NCGL operating system when the conditions which raised alarm XTS331 have been cleared.

Format

The format for log report XTS631 is as follows:

```
Sep 20 14:27:33 cablab.ss.unit1 logman: XTS631 NONE INFO Mate Connectivity
Restored Unit Number : 1, ACTIVE Description : Link0: INSV, mateCon:
AVAIL, netCon: AVAIL; Link1: INSV, mateCon: AVAIL, netCon: AVAIL; PTPLink:
PTP1-SYSB, mateCon: AVAIL;

Sep 20 14:27:34 cablab.ss.unit1 logman: XTS631 NONE INFO Mate Connectivity
Restored Unit Number : 1, ACTIVE Description : Link0: INSV, mateCon:
AVAIL, netCon: AVAIL; Link1: INSV, mateCon: AVAIL, netCon: AVAIL; PTPLink:
BOTH_SYSB, mateCon: AVAIL;

Sep 20 14:27:42 cablab.ss.unit1 logman: XTS631 NONE INFO Mate Connectivity
Restored Unit Number : 1, ACTIVE Description : Link0: INSV, mateCon:
AVAIL, netCon: AVAIL; Link1: INSV, mateCon: AVAIL, netCon: AVAIL; PTPLink:
INSV, mateCon: AVAIL;
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS631	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)

Field	Value	Description
Event Type	Info	The type of trouble or info recorded
Label	Mate Connectivity Restored	Title label for the log
Description	Refer to originating XTS331 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS635

Log report XTS635 is written by the NCGL operating system when the conditions which raised alarm XTS335 have been cleared.

Format

The format for log report XTS635 is as follows:

```
 Apr 29 10:21:53 yang alarmd: XTS635 NONE INFO Link Connectivity Restored
NCGL=yang;Unit=1 Link0: INSV, mateCon: AVAIL, netCon: AVAIL;
Link1: INSV, mateCon: AVAIL, netCon: AVAIL; PTPLink: INSV, mateCon: AVAIL
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman; alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS635	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Link Connectivity Restored	Title label for the log
Description	Refer to originating XTS335 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS636

Log report XTS636 is written by the NCGL operating system when the conditions which raised alarm XTS336 have been cleared.

Format

The format for log report XTS636 is as follows:

```
May 11 09:52:00 cablab alarmd: XTS636 NONE INFO Network Connectivity
Restored NCGL=cablab.ss.unit1;Unit=1 Link0: INSV, mateCon: AVAIL, netCon:
AVAIL;Link1: INSV, mateCon: AVAIL, netCon: AVAIL;  PTPLink: INSV, mateCon:
AVAIL
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS636	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Network Connectivity Restored	Title label for the log
Description	Refer to originating XTS336 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS651

Log report XTS651 is written by the NCGL operating system when the conditions which raised alarm XTS351 have been cleared.

Format

The format for log report XTS651 is as follows:

```
Sep 21 09:31:02 cablab.ss.unit0 alarmd: XTS651 NONE INFO Mate
Communication Restored NCGL=cablab.ss.unit0;Unit=0 Mate unit is available.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman; alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS651	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Mate Communication Restored	Title label for the log
Description	Refer to originating XTS351 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS655

Log report XTS655 is written by the NCGL operating system when the conditions which raised alarm XTS355 have been cleared.

Format

The format for log report XTS655 is as follows:

```
Apr 29 14:11:38 yang logman: XTS655 NONE INFO Release Jam on Inactive unit
Unit Number : 1, UNDETERMINED
Description : Inactive not JAMMED
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS655	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Release Jam on Inactive unit	Title label for the log
Description	Refer to originating XTS355 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS670

Log report XTS670 is written by the NCGL operating system when a SwAct of the system has been initiated.

Format

The format for log report XTS670 is as follows:

```
Apr 8 09:19:33 sp2k-1 logman: XTS670 NONE INFO SWACT Failover Started
Unit Number : 0, ACTIVE
Description : SWACT failover has been initiated. Initiator: Manual
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS670	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	SWACT Failover Started	Title label for the log
Description	SWACT failover has been initiated. Initiator: Manual	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS671

Log report XTS671 is written by the NCGL operating system when a SwAct of the system has been completed.

Format

The format for log report XTS671 is as follows:

```
Apr 8 09:19:33 sp2k-1 logman: XTS671 NONE INFO SWACT Failover Finished
Unit Number : 0, INACTIVE
Description : Result: Passed, Initiator: Manual
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS671	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	SWACT Failover Finished	Title label for the log
Description	Result: Passed, Initiator: Manual	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS691

Log report XTS691 is written by the NCGL operating system when the conditions which raised alarm XTS391 have been cleared.

Format

The format for log report XTS691 is as follows:

```
Apr 29 10:55:48 yang alarmd: XTS691 NONE INIT Array Rebuilt
NCGL=yang;Unit=1; Array: '/dev/md1' (ntvg) The array has been rebuilt.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS691	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Array Rebuilt	Title label for the log
Description	Refer to originating XTS391 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS692

Log report XTS692 is written by the NCGL operating system when the conditions which raised alarm XTS392 have been cleared.

Format

The format for log report XTS692 is as follows:

```
Apr 29 10:55:48 yang alarmd: XTS692 NONE INIT Self Test Device Clear
Apr 29 12:36:39 yin alarmd: XTS692 NONE FAIL Chassis OK NCGL=yin;Unit=0;
Power overload detected.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS692	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Self Test Device Clear	Title label for the log
Description	Refer to originating XTS392 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS695

Log report XTS695 is written by the NCGL operating system when the conditions which raised alarm XTS395 have been cleared.

Format

The format for log report XTS695 is as follows:

```
May 11 09:56:39 yin alarmd: XTS695 NONE THR Threshold exceeded
or Filesystem Error
NCGL=yin;Unit=0; Status: Alarm cleared.
Filesystem is < /tmp >. Used filesystem percentage is 0.50.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS695	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Memory Alarm Cleared	Title label for the log
Description	Refer to originating XTS395 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

USP398

Log report USP398 indicates an SNMP timeout in a USP device.

Note: Log report USP398 is related to the Integrated Element Management Server (IEMS).

Format

The format for log report USP398 is as follows:

```
COMPACT06BT ** USP398 Jan20 12:10:29 0022 FLT USP Fault
Location: 47.135.60.201
Notification Id: 526
State: Raised
Category: processingError
Cause: applicationSubsystemFailure(2)
Time: Jan 20 07:10:29 2004
Component Id: USP=autoimage;Shelf=0;Slot=15;ContextID=0x0
Specific Problem: Log GroupID=13;Log Group=System Node
Maintenance;Log Number=3
Description: Transition to DISABLED Operational State.
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

USP399

Log report USP399 clears all other USP logs.

Note: Log report USP399 is related to the Integrated Element Management Server (IEMS).

Format

The format for log report USP399 is as follows:

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.