Succession Fault Management Logs Reference (volume 3)

ATTENTION
The Succession 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:

- 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 4)

Log ID	Description
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

IEMS logs (Sheet 2 of 4)

Log ID	Description
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
EMJS841	Indicates that the alarm threshold has returned to normal
EMSS 300	Indicates that the client-side Pam + Radius SPI is unable to communicate with the server-side Radius interface
EMSS 301	Indicates that there are problems with the server-side Radius proxy
EMSS 302	Indicates that the IS PAM+ Plug-in fails to communicate with the Integrated EMS SPI
EMSS 303	Indicates that the pam_radius_auth cannot establish or maintain a communications session with the group daemon on the client machine
EMSS 305	Indicates that the Identity Server (IS_ PAM+ Plug-in fails to communicate with the Integrated EMS SPI
EMSS 306	Indicates that a packet from the Radius server is corrupted
EMSS 307	Indicates that a packet from the Radius server has failed verification
EMSS 308	Indicates that the client-side PAM+ Radius SPI is unable to communicate with the Radius Identity Server
EMSS 309	Indicates that a packet from the Radius server does not contain all required fields
EMSS 310	Indicates that the client configuration file cannot be opened
EMSS 311	Indicates that the PAM+ Radius SPI is unable to communicate with the Radius Identity Server

IEMS logs (Sheet 3 of 4)

Log ID	Description
EMSS 312	Indicates that the client-side PAM+ Radius SPI is unable to update file systems
PAM+ Radius SPI User Credential has Expired	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
PAM+ Radius SPI User Account has Expired	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

IEMS logs (Sheet 4 of 4)

Log ID	Description
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
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
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

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

Media Server 2000 logs (Sheet 2 of 2)

Log ID	Description
AMS304	Indicates a feature key error on the Media Server 2000 node
AMS305	Indicates board call resource alarm on the Media Server 2000 node
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”
AMS500	Indicates a board started condition on the Media Server 2000 node
AMS501	Indicates an admin state change on the Media Server 2000 node

Session Server

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

Session Server logs (Sheet 1 of 4)

Log ID	Description
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
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
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
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

Session Server logs (Sheet 2 of 4)

Log ID	Description
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
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
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
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

Session Server logs (Sheet 3 of 4)

Log ID	Description
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
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
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

Session Server logs (Sheet 4 of 4)

Log ID	Description
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
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.*

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:

```
<CLLI>     EMJS340 MMMdd hh:mm:ss #### TBL IEMS OM Collection
          Job Alarm
          Location:<IP address>
          Job Instance:<job name>
          State:<Raise/Clear>
          Category:processingError
          Cause: underlyingResourceUnavailable
          ComponentId:EMS-IEMS=<IPaddress>;Software=<job
          name>;
          Time: Mmm dd hh:mm:ss yyyy
          Description: <variable length string>
```

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	character string	Indicates the state of the log.
Time	character string	Indicates the date and time of the log.
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.

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:

```
<CLLI> EMJS341 MMMDD hh:mm:ss #### TBL IEMS OM Collection Job Status
    Location: <IP address>
    Job instance: <job name>
    State: Raise
    Category: other
    Cause: communicationsSubsystemFailure
    ComponentID: EMS-IEMS=<IP address>, Software=<job name>
    Time: <Mmm dd hh:mm:ss yyyy>
    Description: Collection job <component> 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.
Component Id	character string	Indicates the details of the component.

Action

Refer to 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.

EMJS350

Log report EMJS350 indicates the state of the FTP connection with the device.

The Integrated EMS generates log report EMJS350.

Format

The format for log report EMJS350 is as follows:

```
<CLLI> * EMJS350 MMMDD hh:mm:ss #### TBL IEMS OM Processing Job Alarm
     Location: <IP address>
     Job instance: <job name>
     State: <Raise/Clear>
     Category: processing Error
     Cause: underlyingResourceUnavailable
     ComponentID: IEMS=<IP address>,Software=<job name>;
     Time: <Mmm dd hh:mm:ss yyyy>
     Description: <variable character string>
```

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.
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

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.

EMJS360

Log report EMJS360 indicates the state of a report file.

The Integrated EMS generates log report EMJS360.

Format

The format for log report EMJS360 is as follows:

```
 EMJS360 mmmdd hh:mm:ss
 Location: <IP address>
Job instance: <job name>
State: <Raise, Clear>
Category: processing Error
 Component Id: <IP address, Software>
 Time: <Jun 30 11:09:16 2004>
 FileName: <file name>
Probable cause: File Error
Description: <Error occurred while generating a file or Report
 file generation success.>
```

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	character string	Indicates the state of the job report.
Component Id	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 requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS371

Log report EMJS371indicates that no file is available to transfer.

The Integrated EMS generates log report EMJS371.

Format

The format for log report EMJS371 is as follows:

```
<CLLI> EMJS371 MMMDD hh:mm:ss #### FLT IEMS OM Transfer Job Status
       Location: <IP address>
       Job instance: <job name>
       State: <Raise/Clear>
       Category: communications
       ComponentID: EMS-IEMS=<IP address>,Software=<job name>;
       Time: <Mmm dd hh:mm:ss yyyy>
       Description: <variable length string>
       File Name:<file name>
       Destination: <IP address>
```

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.
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

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.

EMJS540

Log report EMJS540 indicates the status of a job.

The Integrated EMS generates log report EMJS540.

Format

The format for log report EMJS540 is as follows:

```
<CLLI> EMJS540 #### <STATUS> OM Collection Job Status
  Location: <IP address>
  Job Instance: <job name>
  State: <Resumed/Enabled/Disabled/Suspended>
  Category: other
  ComponentID:EMS-IEMS=<IP address>,Software=<job name>;
  Time: <Mmm dd hh:mm:ss yyyy>
```

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	character string	Indicates the state of the job.
Time	character string	Indicates the date and time of the log.
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.

EMJS560

Log report EMJS560 indicates that the state of the Report Job.

The Integrated EMS generates log report EMJS560.

Format

The format for log report EMJS560 is as follows:

```
<CLLI>   EMJS560 MMMDD hh:mm:ss #### OFFL Report Job Status
       Location: <IP address>
       Job Instance:<job name>
       State: <Suspended/Resumed/Disabled/Enabled>
       Category: other
       ComponentID: EMS-IEMS=<IP address>,Software=<job name>
       Time: Mmm dd hh:mm:ss yyyy
```

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	character string	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 that the transfer job has resumed.

The Integrated EMS generates log report EMJS570.

Format

The format for log report EMJS570 is as follows:

```
<CLLI> EMJS570 MMMDD hh:mm:ss #### <STATE> OM Collection Job Status
          Location: <IP address>
          Job instance: <job name>
          State: <Resumed/Enabled/Disabled/Suspended>
          Category: other
          ComponentID:EMS-IEMS=<IP address>,Software=<job name>;
          Time: <Mmm dd hh:mm:ss yyyy>
```

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.
Time	character string	Indicates the date and time of the log.
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 indicates that an SNMP OID mismatch has occurred.

The Integrated EMS generates log report EMJS640.

Format

The format for log report EMJS640 is as follows:

```
<CLLI> EMJS640 MMMDD hh:mm:ss #### INFO IEMS OM Collection Job Status
       Location:<IP address>
       Job instance:<job name>
       State:Info
       Category:processingError
       Cause: datasetProblem
       ComponentID:EMS-IEMS=<IP address>,Software=<job name>;
       Invalid OID List:<integer string>
       Time: <Mmm dd hh:mm:ss yyyy>
       Description:SNMP OID data collection failure for <component name>
```

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.
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.

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:

```
<CLLI> EMJS641 MMMDD hh:mm:ss #### INFO IEMS OM Collection Job Status
          Location:<IP address>
          Job instance:<job name>
          State:Successful
          Category:other
          ComponentID:EMS -IEMS=<IP address>,Software=<job name>;
          Time:<Mmm dd hh:mm:ss yyyy>
          Description:Processing successfully done for the MOs:<device
          details>
```

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.
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.

EMJS642

Log report EMJS642 indicates the partial completion of an SNMP data collection job.

The Integrated EMS generates log report EMJS642.

Format

The format for log report EMJS642 is as follows:

```
<CLLI> EMJS642 MMMDD hh:mm:ss #### INFO IEMS OM Collection Job Status
       Location: <IP address>
       Job instance: <job name>
       State:Incomplete
       Category:other
       ComponentID:EMS-IEMS=<IP address>,Software=<job name>;
       Time: <Mmm dd hh:mm:ss yyyy>
       Description: Collection job <component name> unable to collect
       all attributes. Refer to the perf_log.txt debug log file on the
       Integrated EMS 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.
Time	character string	Indicates the date and time of the log.
Component Id	character string	Indicates the details of the component.

Action

Refer to the perf_log.txt debug log file 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.

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:

```
<CLLI> EMJS651 MMMDD hh:mm:ss #### INFO IEMS OM Processing Job Status
       Location: <IP address>
       Job instance: <job name>
       State: Successful
       Category: other
       ComponentID: EMS-IEMS=<IP address>,Software=<job name>;
       Time: <Mmm dd hh:mm:ss yyyy>
       Description:Processing successfully done for the MOs: <list of
       devices included for the collection>
```

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.
Time	character string	Indicates the date and time of the log.
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 indicates the state of the CSV data collection job.

The Integrated EMS generates log report EMJS652.

Format

The format for log report EMJS652 is as follows:

```
<CLLI> EMJS652 MMMDD hh:mm:ss #### INFO IEMS OM Processing Job Status
         Location: <IP address>
         Job Instance: <job name>
         State: <state of job>
         Category: other
         ComponentID: EMS-IEMS=<IP address>,Software=<job name>;
         Time: <Mmm dd hh:mm:ss yyyy>
         Description: Invalid file format
         File Name: <variable character string>
```

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	character string	Indicates the state of the job (incomplete or failed).
Component Id	character string	Indicates the details of the component.
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.

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:

```
<CLLI> EMJS661 MMMDD hh:mm:ss #### INFO IEMS OM Report Job Status
     Location: <IP address>
     Job instance: <job name>
     State: Successful
     Category: other
     ComponentID:EMS-IEMS=<IP address>,Software=<job name>;
     Time: <Mmm dd hh:mm:ss yyyy>
     Description: <file path>
```

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.
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.

EMJS662

Log report EMJS662 indicates the state of a report job.

The Integrated EMS generates log report EMJS662.

Format

The format for log report EMJS662 is as follows:

```
 EMJS662 mmmdd hh:mm:ss
 Location: <IP address>
Job instance: <job name>
 State: <state of job>
Category: other
 Component Id: <IP address, Software>
 Equipment identifier: <IP address>
Time: <Jun 30 11:09:16 2004>
```

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	character string	Indicates the state of the job - Incomplete or Failure.
Time	character string	Indicates the date and time of the log.
Component Id	character string	Indicates the details of the component.
Equipment identifier	IP address	Indicates the hostname on which the Integrated EMS server is 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.

EMJS671

Log report EMJ 671 indicates the status of a transfer job.

The Integrated EMS generates log report EMJS671.

Format

The format for log report EMJS671 is as follows:

```
<CLLI> EMJS671 MMMDD hh:mm:ss #### INFO IEMS OM Transfer Job Status
    Location: <IP address>
    Job instance: <job name>
    State: Successful
    Category: other
    ComponentID: EMS-IEMS=<IP address>,Software=<job name>;
    Time:<Mmm dd hh:mm:ss yyyy>
    Description:<variable character string>
    File Name: <file name>
    Destination: <IP address>
```

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.
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:

```
<CLLI> EMJS672 MMMDD hh:mm:ss #### TBL IEMS OM Transfer Job Status
        Location: <IP address>
        Job instance: <job name>
        State:Incomplete
        Category:other
        ComponentID:EMS-IEMS=<IP address>,Software=<job name>;
        Time:<Mmm dd hh:mm:ss yyyy>
        File Name: <file name>
        Destination:<IP address>
```

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.
Time	character string	Indicates the date and time of the log.
Component Id	character string	Indicates the details of the component.
Equipment identifier	IP address	Indicates the hostname on which the Integrated EMS server is running.
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 indicates that an alarm threshold has reached the maximum value.

The Integrated EMS generates log report EMJS840.

Format

The format for log report EMJS840 is as follows:

```
<CLLI>   EMJS840 MMMDD hh:mm:ss #### TBL Threshold Alarm
   Location: <IP address>
   Job Instance:<job name>
   Time: <Mmm dd hh:mm:ss yyyy>
   State: Critical
   Category: other
   Cause: Threshold Alarm
   ComponentID: EMS-IEMS=<IP address>,Software=<job name>;Node=<node ID>
   Monitored Value : <OID>
   Collected Value: <collected value>
   Threshold type: <threshold type>
   Threshold: <threshold value>
   Rearm Value: <rearm value>
   Description: Threshold reached the max value
```

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.
Collected Value	integer	Indicates the actual value collected from the device for this OID.

Field	Value	Description
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 EMJS841 indicates that the alarm threshold has returned to normal.

The Integrated EMS generates log report EMJS841.

Format

The format for log report EMJS841 is as follows:

```
<CLLI>   EMJS841 MMMDD hh:mm:ss #### TBL Threshold Alarm
       Location: <IP address>
       Job Instance:<job name>
       Time: <Mmm dd hh:mm:ss yyyy>
       State: Clear
       Category: other
       Cause: Threshold Alarm
       ComponentID: EMS-IEMS=<IP address>,Software=<job
       name>;Node=<node ID>
       Monitored Value : <OID>
       Collected Value: <collected value>
       Threshold type: <threshold type>
       Description: 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 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.

EMSS 300

Log report EMSS 300 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 via the standard UNIX syslog C API.

The Integrated EMS generates log report EMSS 300.

Format

The format for log report EMS 300 is as follows:

```
mmmdd hh:mm:ss host1 pam_radius_auth.so:EMSS300 MAJOR FLT EMSS
Location: <CLIENT - hostname>
Time: <Jun 30 11:09:16 2003>
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
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 that there is 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.

EMSS 301

Log report EMSS 301 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 EMSS 301.

Format

The format for log report EMS 301 is as follows:

```
mmmdd hh:mm:ss host1 RADSVR:_V2_~I=<IP address>
~H=host1~A=RADSVR~S=0000~~EMSS301 MAJOR FLT
<Device name:device port> EMSS
Location: <SERVER - hostname>
Time: <Jun 30 11:09:16 2003>
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
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.

EMSS 302

Log report EMSS 302 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 EMSS 302.

Format

The format for log report EMS 302 is as follows:

```
mmmdd hh:mm:ss host1 RADSVR: _V2_~I=<IP address>
~H=host1~A=RADSVR-S=0000~~EMSS302 MINOR FLT
<Device name:device port> EMSS
Location: <SERVER - hostname>
Time: <Jun 30 11:09:16 2003>
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
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.

EMSS 303

Log report EMSS 303 indicates a communication failure with the PAM+ Radius group daemon. This log indicates that the pam_radius_auth cannot establish or maintain a communications session with the group daemon on the client machine.

Note: Log report EMSS 303 is sent directly to syslog via the standard UNIX syslog C API.

The Integrated EMS generates log report EMSS 303.

Format

The format for log report EMS 303 is as follows:

```
mmmddhh:mm:ss host1 pam_radius_auth.so: EMSS303 MAJOR FLT EMSS
Location: <Client - hostname>
Time: <Jun 30 11:09:16 2003>
Category: communicationsAlarm
Probable Cause: connectionEstablishmentError
Component Id: PAM+ Radius SPI
Description: Communication failure with the PAM+ RADIUS
group daemon.
Recovery Action: Please verify the PAM+ RADIUS group daemon
is running on the client machine.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time	character string	Indicates the date and time of the log.
Client - hostname	character string	Indicates the client and hostname.

Action

Make sure that the group daemon is running.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS 305

Log report EMSS 305 indicates that the client side PAM+ Radius SPI is unable to communicate with the server-side Radius interface.

The Integrated EMS generates log report EMSS 305.

Format

The format for log report EMS 305 is as follows:

```
mmmddhh:mm:ss host1 pam_radius_auth.so: EMSS305 MAJOR FLT EMSS
Location: <SERVER - hostname>
Time: <Jun 30 11:09:16 2003>
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
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.

EMSS 306

Log report EMSS 306 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 EMSS 306 is sent directly to syslog via the standard Unix syslog C API.

The Integrated EMS generates log report EMSS 306.

Format

The format for log report EMS 306 is as follows:

```
mmmdd hh:mm:ss host1 pam_radius_auth.so: EMSS306 MAJOR FLT EMSS
Location: <SERVER - hostname>
Time: <Jun 30 11:09:16 2003>
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
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.

EMSS 307

Log report EMSS 307 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 EMSS 307 is sent directly to syslog via the standard Unix syslog C API.

The Integrated EMS generates log report EMSS 307.

Format

The format for log report EMS 307 is as follows:

```
mmmdd hh:mm:ss host1 pam_radius_auth.so: EMSS307 MAJOR FLT EMSS
Location: <SERVER - hostname>
Time: <Jun 30 11:09:16 2003>
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
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.

EMSS 308

Log report EMSS 308 indicates that the client-side PAM+ Radius SPI is unable to communicate with the Radius Identity Server.

Note: Log report EMSS 308 is sent directly to syslog via the standard Unix syslog C API.

The Integrated EMS generates log report EMSS 308.

Format

The format for log report EMS 308 is as follows:

```
mmmdd hh:mm:ss host1 pam_radius_auth.so: EMSS308 MAJOR FLT EMSS
Location: <SERVER - hostname>
Time: <Jun 30 11:09:16 2003>
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
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.

EMSS 309

Log report EMSS 309 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 EMSS 309 is sent directly to syslog via the standard Unix syslog C API.

The Integrated EMS generates log report EMSS 309.

Format

The format for log report EMS 309 is as follows:

```
mmmdd hh:mm:ss host1 pam_radius_auth.so: EMSS309 MAJOR FLT EMSS
Location: <SERVER - hostname>
Time: <Jun 30 11:09:16 2003>
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
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.

EMSS 310

Log report EMSS 310 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 EMSS 310 is sent directly to syslog via the standard Unix syslog C API.

The Integrated EMS generates log report EMSS 310.

Format

The format for log report EMS 310 is as follows:

```
mmmdd hh:mm:ss host1 pam_radius_auth.so: EMSS310 MAJOR FLT EMSS
Location: <SERVER - hostname>
Time: <Jun 30 11:09:16 2003>
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
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.

EMSS 311

Log report EMSS 311 indicates that the PAM+ Radius SPI is unable to communicate with the Radius Identity Server.

Note: Log report EMSS 311 is sent directly to syslog via the standard Unix syslog C API.

The Integrated EMS generates log report EMSS 311.

Format

The format for log report EMS 311 is as follows:

```
mmmdd hh:mm:ss host1 pam_radius_auth.so: EMSS311 MAJOR FLT EMSS
Location: <SERVER - hostname>
Time: <Jun 30 11:09:16 2003>
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
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.

EMSS 312

Log report EMSS 312 indicates that the client-side PAM+ Radius SPI is unable to update file systems.

Note: Log report EMSS 312 is sent directly to syslog via the standard Unix syslog C API.

The Integrated EMS generates log report EMSS 312.

Format

The format for log report EMS 312 is as follows:

```
mmmdd hh:mm:ss host1 pamrad_daemon: EMSS312 MAJOR FLT EMSS
Location: <SERVER - hostname>
Time: <Jun 30 11:09:16 2003>
Category: processingErrorAlarm
Probable Cause: applicationSubsystemFailure
Component Id: PAM+ Radius SPI
Description: Message: Daemon has failed to update system files on
client machine.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
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.

PAM+ Radius SPI User Credential has Expired

This log report (formerly EMSS 313) 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.

Note: This log report is sent directly to syslog via the standard Unix syslog C API.

The Integrated EMS generates log report "PAM+ RADIUS SPI User Credential has Expired".

Format

The format for this log report is as follows:

```
mmmdd hh:mm:ss host1 pam_radius_auth.so: Authentication failed:
Password for user <user name> has expired
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
user name	character string	Indicates the user name.

Action

The user must update their password on the central security server.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

PAM+ Radius SPI User Account has Expired

This log report (formerly EMSS 314) 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.

Note: This log report is sent directly to syslog via the standard Unix syslog C API.

The Integrated EMS generates log report "PAM+ RADIUS SPI User Account has Expired".

Format

The format for this log report is as follows:

```
mmmdd hh:mm:ss host1 pam_radius_auth.so: Authentication failed:
Account for user <user name> has expired.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
user name	character string	Indicates the user name.

Action

If the user account is still required, the user account must be reset on the central security server.

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 there is a failure to initialize the single sign on (SSO) facility. SSO tokens will not be generated.

The Integrated EMS generates log report EMSS320.

Format

The format for log report EMSS320 is as follows:

```
 EMSS320 mmmdd hh:mm:ss NONE INFO <Device name:device port>
Location: <SERVER - hostname>
Time: <Jun 30 11:09:16 2004>
Category: processingErrorAlarm
 Probable Cause: configurationOrCustomizationError
 Component Id: PAM Proxy
 Description: Failed to initialize single sign on facility.
 SSO tokens will not be generated.
 Recovery Action: Configure and start the Sun One Identity
 server, then restart the Tomcat servlet engine.
```

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.
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 there is a failure to authenticate the user due to an unhandled internal error.

The Integrated EMS generates log report EMSS321.

Format

The format for log report EMSS321 is as follows:

```
 EMSS321 mmmdd hh:mm:ss NONE INFO <Device name:device port>
Location: <SERVER - hostname>
Time: <Jun 30 11:09:16 2004>
Category: processingErrorAlarm
 Probable Cause: softwareProgramError
 Component Id: PAM Proxy
 Description: Could not authenticate user due to unhandled
 internal error.
Recovery Action: Inspect the state of the centralized security
 server components.See debug logs in <filepath debug logs>.
```

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.
Location	character string	Indicates the server and hostname.
Time	character string	Indicates the date and time of the log.
Debug logs	character string	Indicates the file path of the debug logs.out file.

Action

Inspect the state of the centralized security server components. See the debug logs.

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 that no single-sign-on token is available after authentication.

The Integrated EMS generates log report EMSS322.

Format

The format for log report EMSS322 is as follows:

```
 EMSS322 mmmdd hh:mm:ss NONE INFO <Device name:device port>
Location: <SERVER - hostname>
Time: <Jun 30 11:09:16 2004>
Category: processingErrorAlarm
 Probable Cause: outOfService
 Component Id: PAM 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
Device name:device port	character string	Indicates the device name and device port.
Location	character string	Indicates the server and hostname.
Time	character string	Indicates the date and time of the log.

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.

EMSS323

Log report EMSS323 indicates that no single-use tokens are generated due to an unhandled internal error.

The Integrated EMS generates log report EMSS323.

Format

The format for log report EMSS323 is as follows:

```
 EMSS323 mmmdd hh:mm:ss NONE INFO <Device name:device port>
Location: <SERVER - hostname>
Time: <Jun 30 11:09:16 2004>
Category: processingErrorAlarm
 Probable Cause: softwareProgramError
 Component Id: PAM Proxy
 Description: Could not generate single-use tokens due to
 unhandled internal error.
Recovery Action: Inspect the state of the centralized security
 server components. See debug logs in <filepath debug logs>.
```

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.
Location	character string	Indicates the server and hostname.
Time	character string	Indicates the date and time of the log.
Debug logs	character string	Indicates the file path of the debug logs.out file.

Action

Check the status of the centralized security server. See the debug logs.

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 that the UNIX user's profile cannot be read due to an unhandled internal error.

The Integrated EMS generates log report EMSS324.

Format

The format for log report EMSS324 is as follows:

```
 EMSS324 mmmdd hh:mm:ss NONE INFO <Device name:device port>
Location: <SERVER - hostname>
Time: <Jun 30 11:09:16 2004>
Category: processingErrorAlarm
 Probable Cause: softwareProgramError
 Component Id: PAM Proxy
 Description: Could not read unix user's profile due to
 unhandled internal error.
Recovery Action: Inspect the state of the centralized security
 server components. See debug logs in <filepath debug logs>.
```

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.
Location	character string	Indicates the server and hostname.
Time	character string	Indicates the date and time of the log.
Debug logs	character string	Indicates the file path of the debug logs.out file.

Action

Check the status of the centralized security server. See the debug logs.

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:

```
<CLLI> *** IEMS398 MMMDD hh:mm:ss #### FLT Communication Lost
    Location: <IP address>
    Motification ID: <variable length integer>
    State: Raised
    Category:Communications
    Cause: Communications subsystem failure
    Time: <Mmm dd hh:mm:ss yyyy>
    ComponentId: <component name of the device>
    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 event source.
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 no associated OM registers.

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:

```
<CLLI> *** IEMS399 MMMDD hh:mm:ss #### FLT Communication Regained
   Location: <IP address>
   Notification ID: <variable length integer>
   State: Cleared
   Category: Communications
   Time: <Mmm dd hh:mm:ss yyyy>
   Component Id: <component name of the device>
   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	character string	Indicates the IP address of the event source.
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 indicates events raised from unknown devices.

The Integrated EMS generates log report IEMS601.

Format

The format for log report IEMS601 is as follows:

```
<CLLI>   IEMS601 MMMDD hh:mm:ss #### INFO
        Location: <IP address of the event source>
        Event:    <OID>
        Varbind0: <OID value>
        Varbind1: <OID value>
        Varbind2: <OID value>
        Varbind3: <OID value>
```

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.

IEMS602

Log report IEMS602 indicates events raised from a known device.

The Integrated EMS generates log report IEMS602.

Format

The format for log report IEMS602 is as follows:

```
<CLLI>   IEMS602 MMMDD hh:mm:ss #### INFO Fault
         Location: <IP address of the event source>
         Event:    <OID>
         Varbind0: <OID value>
         Varbind1: <OID value>
         Varbind2: <OID value>
         Varbind3: <OID value>
```

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.

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 indicates missed notifications.

The Integrated EMS generates log report IEMS603.

Format

The format for log report IEMS603 is as follows:

```
<CLLI>   IEMS603 MMMDD hh:mm:ss #### INFO Fault
        Location: <IP address of the event source>
        Component Id: <component name of the device>
        Time: <mmm dd hh:mm:ss yyyy>
        Description: Notification(s) missed in ML 29 - 29
```

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 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:

```
<CLLI>   IEMS604 MMMDD hh:mm:ss #### INFO Fault
       Location: <IP address>
       Notification Id:<notification Id>
       State: Cleared
       Time: <Mmm dd hh:mm:ss yyyy>
       ComponentId: <component name of the device>
       Description: <variable length string>
       Web Monitor: Alarm cleared by TSSAlarmManager as requested
```

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.
Notification Id	character string	Indicates the notification Id .
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.

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:

```
<CLLI>   IEMS606 MMMDD hh:mm:ss #### INFO Database Fault
       Location: <IP address>
       State: INFO
       Time: <Mmm dd hh:mm:ss yyyy>
       Maximum No.of Event <number of events allowed before an event is
       generated>
       Event count: <event count>
       Description: <variable length string>
```

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 which will be deleted by the DB cleanup job.

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 beween 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:

```
<CLLI>   IEMS607 MMMDD hh:mm:ss #### INFO IEMS Autogenerated Clear
       Location: <location field value>
       NotificationID: <notification Id field value>
       State: Clear
       Time: <Mmm dd hh:mm:ss yyyy>
       Specific Problem: <specific problem or fault code>
       Category: <alarm category>
       Component Id: <component Id field value>
       Description: Raised log: ABCD123; <variable length string>
```

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.
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.

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.

AMS500

Log report AMS500 indicates a board started condition on the Media Server 2000 node. The IPM-1610 or TP-6310 board was restarted.

Format

Board Started - associated trap is <acBoardEvBoardStarted>

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action. This is an information log.

Associated OM registers

This log report has no associated OM registers.

Additional information

There is no corresponding clear SNMP trap. This is not an alarm and does not go in the active alarm table. This trap is a signal to clear the entire active alarm table.

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.

DBSE300

Log report DBSE300 is generated any time a change in database connectivity is detected, specifically a loss of connectivity between the Session Server 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 recorded

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

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 recorded
Label	Alphanumeric	Title label for the log
Description	All SIP Incoming Msgs Blocked	Detailed description of the trouble

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 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.

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
```

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	SIPC310	The component prefix and number of the log
Severity	critical	The log severity (may be related to alarm severity)
Event Type	Trouble	The type of trouble recorded
Label	SIP CallP	Title label for the log
Description	No Database Connection	See a detailed description of the trouble in the log details.

Action

Reestablish 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.

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 recorded

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

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 recorded
Label	Alphanumeric	Title label for the log
Description	No Data Found	Detailed description of the trouble

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 recorded

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

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 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; 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 critical alarm SIPM301 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 SIPM301 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 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 lowered 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 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 SIPM500 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 recorded
Label	SIP Maintenance State Change	Title label for the log
Description	Alphanumeric	Detailed description of the trouble; see section: Additional information on page 119

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

STGW700

Log report STGW700 is an information log that is generated by the SIP Gateway Call Processing Application.

This log may be generated when callp activity is interrupted or negatively impacted, such as during a Session Server 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
```

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	SIPGW700	The component prefix and number of the log

Field	Value	Description
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	The type of trouble recorded
Label	sipcallp; linkmtc	Title label for the log
Description	LogMessage	Detailed description of the messages, refer to section Additional information.

Action

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

Associated OM registers

This log report has no associated OM registers.

Additional information

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

- 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, 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 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 for a description of how to monitor the connectivity and network status for both Session Server 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 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 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 for a description how to monitor the status of CPU and memory related resources for the active Session Server 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 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 for a description how to monitor the status of disk drive resources for the active Session Server 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 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 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 for a description how to monitor the status of zombie processes for the active Session Server 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.

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 platform generates log report XTS305 in addition to the alarm.

Format

The format for log report XTS305 is as follows:

```
APR17 08:09:54 ngss-1 XTS305 minor FLT  NTP Error
Unit Number : 0, ACTIVE
Host is not communicating with any NTP
              server(s); No. of configured server(s): 2; 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	N/A	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 recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble

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 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 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 for a description how to monitor the status of CPU and memory related resources for the active Session Server 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 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 recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble

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 for a description how to reboot the affected unit. After the reboot, check the resulting system status in *Session Server Fault Management*, NN10332-911

If the alarm persists, consider replacing the Session Server 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 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 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 for a description how to monitor the status of the application on both Session Server 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.

XTS316

Log report XTS316 indicates that the standby call processing application on the inactive Session Server is out of service and the Session Server node is not operation in a fault-tolerant mode.

The Session Server platform generates log report XTS316 in addition to the alarm.

Format

The format for log report XTS316 is as follows:

```
APR7 08:16:22 ngss-1 XTS316 major FLT Application Out-of-Serv
Unit Number : 0, ACTIVE
The application state has changed from In
Service to Out Of Service.
```

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	XTS316	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 for a description how to monitor the status of the application on both Session Server 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 active unit cannot communicate to the mate unit through the ethernet connections.

The Session Server 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 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 for a description how to monitor the connectivity and network status for both Session Server 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 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 recorded

Field	Value	Description
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 for a description how to monitor the connectivity and network status for both Session Server 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 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 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 for a description how to monitor the connectivity and network status for both Session Server 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 unit is unavailable or status information for the mate Session Server unit is unavailable at the maintenance interface.

The Session Server 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 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 for a description how to monitor the connectivity status for the active and standby Session Server 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 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 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 for a description how to monitor the status of CPU and memory related resources for the active Session Server 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.

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 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 recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble

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 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 recorded

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

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 recorded
Label	Memory Alarm Cleared	Title label for the log
Description	Refer to originating XTS300 alarm for details	Detailed description of the trouble.

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 recorded
Label	CPU Alarm	Title label for the log
Description	Refer to originating XTS301 alarm for details	Detailed description of the trouble.

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 recorded
Label	Memory Alarm Cleared	Title label for the log
Description	Refer to originating XTS302 alarm for details	Detailed description of the trouble.

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.

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 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 recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble

Action

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

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

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.

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 recorded
Label	Memory Alarm Cleared	Title label for the log
Description	Refer to originating XTS303 alarm for details	Detailed description of the trouble.

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 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.

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 recorded
Label	CPU Utilization Cleared	Title label for the log
Description	Refer to originating XTS306 alarm for details	Detailed description of the trouble.

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 recorded
Label	Hardware Fault Cleared	Title label for the log
Description	Refer to originating XTS309 alarm for details	Detailed description of the trouble.

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 recorded

Field	Value	Description
Label	Duplex Node	Title label for the log
Description	Refer to originating XTS315 alarm for details	Detailed description of the trouble.

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 recorded
Label	Application In-service	Title label for the log
Description	Refer to originating XTS316 alarm for details	Detailed description of the trouble.

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 recorded
Label	Mate Connectivity Restored	Title label for the log
Description	Refer to originating XTS331 alarm for details	Detailed description of the trouble.

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	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 recorded
Label	Link Connectivity Restored	Title label for the log
Description	Refer to originating XTS335 alarm for details	Detailed description of the trouble.

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 recorded
Label	Network Connectivity Restored	Title label for the log
Description	Refer to originating XTS336 alarm for details	Detailed description of the trouble.

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	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 recorded
Label	Mate Communication Restored	Title label for the log
Description	Refer to originating XTS351 alarm for details	Detailed description of the trouble.

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 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.

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 recorded
Label	SWACT Failover Started	Title label for the log
Description	SWACT failover has been initiated. Initiator: Manual	Detailed description of the trouble.

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 recorded
Label	SWACT Failover Finished	Title label for the log
Description	Result: Passed, Initiator: Manual	Detailed description of the trouble.

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 recorded
Label	Array Rebuilt	Title label for the log
Description	Refer to originating XTS391 alarm for details	Detailed description of the trouble.

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 recorded
Label	Self Test Device Clear	Title label for the log
Description	Refer to originating XTS392 alarm for details	Detailed description of the trouble.

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 recorded
Label	Memory Alarm Cleared	Title label for the log
Description	Refer to originating XTS395 alarm for details	Detailed description of the trouble.

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:

```
COMPACT06BT ** USP399 Jan20 12:10:29 0022 FLT USP Fault
Location: 47.135.60.201
Notification Id: 526
State: Cleared
Category: processingError
```

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.