Maintaining and Troubleshooting Avaya Aura™ Session Manager

03-603325
Issue 1.1
Release 1.1
June 2009

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full legal page information, please see the documents, *Avaya Support Notices for Software Documentation*, 03-600758, and *Avaya Support Notices for Hardware Documentation*, 03-600759.

These documents can be accessed on the documentation CD and on the Web site, http://www.avaya.com/support. **On the Web site, search for the document number in the Search box.**

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this Documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Copyright

Trademarks

Avaya, Communication Manager Express, MultiVantage, and INTUITY are trademarks of Avaya Inc. Some MultiVantage Express applications use the Open Source Indy Sockets library. License terms for this library are available at http://www.indyproject.org/License/index.en.iwp.

All non-Avaya trademarks are the property of their respective owners.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information identifying Third Party Components and the Third Party Terms that apply to them is available on Avaya’s web site at: http://support.avaya.com/ThirdPartyLicense/

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your contact center. The support telephone number is 1 800 242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Chapter 1: Maintenance and troubleshooting

This document provides information regarding Avaya Aura^{TM} Session Manager maintenance functions and how to identify, understand, and troubleshoot problems. It provides procedures for backing up and restoring data, shutting down and rebooting the Session Manager host server, running maintenance tests, replacing hardware, how to set up and view SIP tracing, how to monitor system components, and procedures for troubleshooting errors and alarms.

For alarms and trouble reports, technicians should first start their investigation on System Manager and only access Session Manager when required.

Required equipment

For maintenance and troubleshooting activities, you will need:

- A laptop
- SIP Protocol Analyzer
- xming or other virtual desktop tool
- DVD burner
- USB keyboard and mouse
- SVGA monitor
- Network sniffer such as wireshark

Customer account commands

Starting with Service Pack 1, customer account users may run several commands which were previously reserved only for the craft login.

The commands are executed from the shell of the Session Manager system.

The commands which cust account users may execute after Service Pack 1 has been installed are:

- /home/cust/SMnetSetup
- /home/cust/upgradeSM
- /opt/Avaya/bin/start

- /opt/Avaya/bin/restart
- /opt/Avaya/bin/statapp
- /opt/Avaya/bin/swversion
- /opt/Avaya/bin/initTM
- /opt/Avaya/bin/changeMgmtIP
- /opt/Avaya/bin/smconfig
- /opt/Avaya/bin/shutdownSM
- /opt/Avaya/bin/rebootSM

Chapter 2: Accessing Session Manager

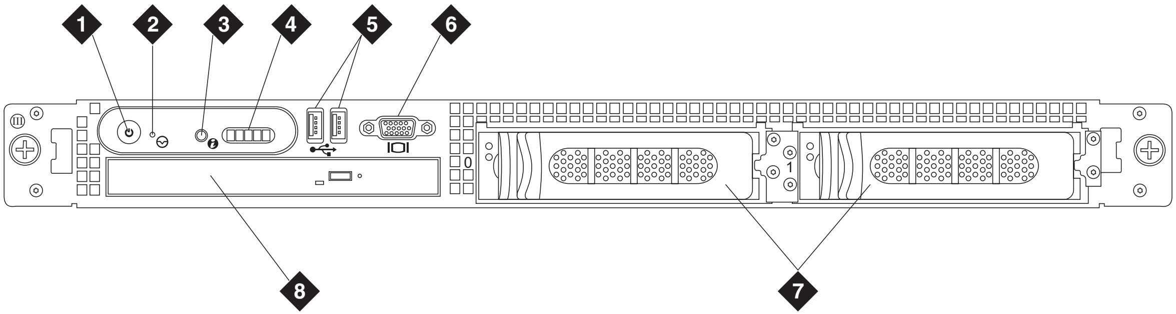
Local access

Access to Session Manager is not really needed except for installations and upgrades.

Local access is provided through each server's services port for installation of the Session Manager and major upgrades.

The following figure shows the front panel of the S8510 server:

Figure 1: Avaya S8510 Server - Front panel



hw8510fn LAO 020108

1.	Power-on indicator, power button	**5.**	USB 2.0 connectors
2.	Nonmaskable Interrupt (NMI) button (disabled)	**6.**	Video connector
3.	System identification button (used to locate equipment within the rack)	**7.**	Hard disk drives
4.	LCD display (system ID, status information, and system error messages)	**8.**	Slimline CD/DVD drive

Using the services port

A USB keyboard, mouse and SVGA monitor can be connected to front panel connectors on the S8510 server faceplate. This can be done instead of connecting a service laptop to the second Ethernet port on the back to access the server locally.

Remote access

Remote access to Session Manager for Release 1.1 is provided by using one of the following access methods:

- RSIG
- SAC/SAC Lite/SSG/SIG
- SSLVPN
- Web Conferencing using Meeting Exchange

A secure shell (ssh) connection between System Manager and any Session Manager is required for shell access.

Chapter 3: Alarming

The Alarming service provides access to alarms generated by the components of a Session Manager system. The following operations can be performed:

- View an alarm
- Change the status of an alarm
- Export alarms to a spreadsheet application file

System Manager generates alarms to notify users of system events. Alarms are classified by their effect on system operation and are grouped by categories. Each alarm category identifies the system component that generates the alarm. If configured, System Manager will forward alarms to Avaya Services. It can also be configured to send SNMP traps to the customer Network Management System.

Alarm severities can be displayed in different colors in the Alarm Table. The colors can be customized using
Settings > Service Profile Management > System Manager 1.0 > Alarming UI

Alarm severities

The alarm severities are:

- CRITICAL alarms indicate that the system or certain system components are unusable. The default color for these alarms is red.
- INDETERMINATE alarms indicate a log event is missing the severity but still matches one of the established alarm rules. This alarm is displayed in blue.
- MAJOR alarms identify failures that cause a critical degradation of service. These alarms require immediate attention. These alarms are displayed in orange.
- MINOR alarms identify failures that cause some service degradation but that do not render a crucial portion of the system inoperable. Minor alarms require attention. However, a minor alarm typically affects only a few trunks, stations, or a single feature. These alarms are displayed in yellow.
- WARNING alarms identify failures that cause no significant degradation of service or equipment failures external to the switch. These failures are not reported to a services organization. These alarms are displayed in purple.

Forwarding alarms to Avaya Enterprise

The setup for alarm forwarding from a System Manager Enterprise to Avaya Production Enterprise is found on the Service Profile Management SPIRIT DataTransport page. The configuration modifications to establish the secure connection require information for the customer's proxy server by entering the correct values for the field described below. Some of the default values can be used for most proxy connections.

To access the Service Profile Management SPIRIT DataTransport page:

1. Click **Settings > Service Profile Management > SPIRIT 1.0 > DataTransportConfig** in the left navigation pane on the System Manager Common Console.
2. Enter information in the fields as follows:

Field	Description
Connection.AvayaProduction.UseProxy	Whether to use proxies for this platform (true or false)
OrganizationFQDN	A Fully Qualified Domain Name to uniquely identify the business organization that the SM100 platform resides in.
ProxyAddress	The domain name or IP address of the proxy to use.
ProxyPass	The password to use with the proxy.
ProxyPort	The port of the proxy to use.
ProxyType	The type of proxy to use (HTTP or SOCKS).
ProxyUseAuthentication	Whether to use username/password authentication with this proxy (true or false).
ProxyUser	The user name to use with the proxy.

Forwarding alarms to NMS

Alarm forwarding from a System Manager Enterprise to a Network Management System (NMS) destination is set up using the Service Profile Management AlarmMgmt page.

To set up NMS alarm forwarding:

1. Click on **Settings > Service Profile Management > AlarmManagementService 1.0 > AlarmMgmt** in the left navigation pane on the System Manager Common Console.

2. Click the **Edit** button and enter the appropriate information in the fields:

Field	Description
nms.forward	Enables/disables Network Management System forwarding. The default is false (disable NMS forwarding).
nms.urls	A comma-separated list of NMS urls. For example: [123.456.78.90:9162]. Note: the [ ] must surround the destination IP address and port

3. Click the **Commit** button when finished.
4. The JBoss needs to be restarted for changes to take effect.

Alarm events

There are three types of alarm event logging:

- ALARM - Software recovery actions have failed to correct the problem.
- WARN - Indicates that something is not quite right. This is not an alarm, but repeated instances may cause it to be an alarm.
- CLEAR - The problem has been fixed and the alarm has been cleared.

Viewing alarms

To view alarms:

1. Click on **Monitoring > Alarming** in the left navigation pane on the System Manager Common Console.
2. Select an alarm by clicking in the box in the first column of an alarm entry or all on the page. You can select multiple alarms.
3. Click on **View**

Filtering alarms

Alarms can be filtered based on status, M/E Reference Number, Agent Reference, or severity. You can use more than one filter criteria on the selected alarms.

To set filters:

1. Click on **Monitoring > Alarming** in the left navigation pane on the System Manager Common Console.
2. On the Alarming page, select the alarms you want to filter.
3. Click on **Filter: Enable**, located at the top right corner of the alarm log table.
4. Select the filter criteria you want to apply to the selected alarms. The **Status** and **Severity** fields have drop-down menus.
5. Click on **Filter: Apply.** A message will be displayed if no records are found which match the specified filter criteria.

Changing alarm status

To change the status of an alarm:

1. Click **Monitoring > Alarming** in the left navigation pane on the System Manager Common Console.
2. On the Alarming page, select an alarm and click **Change Status**
3. Click on the status that you want to apply to the selected alarm.

The status of an alarm can be:

- Acknowledged - Maintenance support must manually set the alarm to this state, indicating the failure is being investigated.
- Clear - Maintenance support must manually set the alarm to this state, indicating that the error condition has been resolved.

Exporting alarms

To export alarms to a csv file to import into Excel or another spreadsheet application:

1. Click **Monitoring > Alarming** in the left navigation pane on the System Manager Common Console.

2. To export a selected alarm to a csv file, select an alarm and click on **More Actions > Export Selected**.

   To export all of the alarms to a csv file, click on **More Actions > Export All**

3. Save the exported file to the local disk.

Searching for alarms

Use the **Advanced Search** function to find alarms based on specified search conditions. After specifying search conditions, the system displays only those alarms which satisfy the search conditions. Multiple search conditions can be specified.

To specify search conditions for alarms:

1. Click **Monitoring > Alarming** in the left navigation pane on the System Manager Common Console.
2. On the Alarming page, click on **Advanced Search**
3. In the “Click to Search to find alarms for the given search conditions”, select the search criterion from each of the drop-down menus.
4. If you want to add another search condition, click on the **+** button and create another search condition.
5. To delete a search condition, click on the **-** button. You can delete a search condition only if you have more than one search condition specified.
6. Select AND or OR from the drop-down list. This option appears when you add a search condition using the **+** button.
7. Click **Search** to find alarms for the given search conditions.

Alarm Event Codes

The table for Alarm Event Codes, their descriptions, and troubleshooting actions is found in Appendix A: Log and Alarm Event IDs.

Chapter 4: Logging

The Logging service provides access to logs generated by the components of a Session Manager system. The Management Console allows you to monitor log messages. You can view the details of a log, perform a search for logs, and filter specific logs. Log details include information about the event that generated the log and severity level of the log. You can search logs based on search conditions and set filters to view logs that match the filter criteria.

Viewing log details

To view logs:

1. Click on **Monitoring > Logging** in the left navigation pane on the System Manager Common Console.
2. Select a log by clicking in the box in the first column of a log entry or all on each page. You can select multiple log entries.
3. Click on **View**

Filtering logs

Log entries can be filtered based on Log ID, Host Name, Product Type, Severity, Event ID, Message, Process Name, or Facility. You can use more than one filter criterion on the selected log entries.

To set filters:

1. Click on **Monitoring > Logging** in the left navigation pane on the System Manager Common Console.
2. On the Logging page, select the logs you want to filter.
3. Click on **Filter: Enable**, located at the top right corner of the log entry table.
4. Enter or select the filter criteria you want to apply to the selected log entries. Several of the column titles have drop-down menus.
5. Click on **Filter: Apply.** A message will be displayed if no records are found which match the specified filter criteria.

Searching for log entries

Use the **Advanced Search** function to find log entries based on specified search conditions. After specifying search conditions, the system displays only those log entries which satisfy the search conditions. Multiple search conditions can be specified.

To specify search conditions for log entries:

1. Click **Monitoring > Logging** in the left navigation pane on the System Manager Common Console.
2. On the Logging page, click on **Advanced Search**
3. In the Criteria section, select the search criterion from each of the drop-down menus.
4. If you want to add another search condition, click on the **+** button and create another search condition.
5. To delete a search condition, click on the **-** button. You can delete a search condition only if you have more than one search condition specified.
6. Select AND or OR from the drop-down list. This option appears when you add a search condition using the **+** button.
7. Click **Search** to find log entries for the given search conditions.

Log Event Codes

The table for Event IDs, their descriptions, and troubleshooting actions are found in Appendix A: Log and Alarm Event IDs.

Chapter 5: Call Detail Recording (CDR)

The Call Detail Recording (CDR) feature records information on tandem calls. The call record contains information regarding:

- time of the call
- duration of the call
- dialed number
- calling party
- terminating SIP entity
- originating SP entity

Minimum requirements

In order to support the Session Manager CDR functionality, the following minimum requirements must be met:

- The Session Manager server must be running the Session Manager first release or a subsequent release.
- There must be IP connectivity between the CDR adjunct and the target server at least from time to time to allow remote collection of the CDR data files.
- The CDR adjunct must be compatible with Session Manager CDR formats. Contact your Avaya representative.

Security provisions

Due to the potentially sensitive nature of CDR records, a secure transport mechanism is used for all communications between the CDR adjunct and the server such as Secure File Transfer Protocol (SFTP). Periodically, the CDR adjunct must log on to each of the administered Session Manager servers and retrieve the CDR data files that are available.

If firewalls are implemented anywhere between the CDR adjunct and the various Session Manager servers, it may be necessary to “punch” pinholes in those firewalls to allow communication between the CDR adjunct and the servers. Please work with the network administrators to implement these pinholes if needed.

CDR description

The CDR records are stored on the server's local hard drive. They are not transmitted over an IP connection to the CDR adjunct. CDR data is transferred in an encrypted manner from the Session Manager server to the CDR adjunct using a secure file transfer protocol such as SFTP. CDR records are stored and transferred in batches rather than one record at a time.

When CDR is enabled, the CDR records are saved in a special directory on the server's hard drive.

The CDR adjunct retrieves the CDR data files by logging into the server and copying the files to its own storage device. The CDR adjunct uses a special login and password that the server administrator has created just for this purpose. This login is restricted to only accessing the directory where the CDR records are stored. After all of the files are successfully copied, the CDR adjunct deletes the files from the server's hard drive and processes the CDR records.

There are three methods for removing CDR data files from the server, listed in order of preference:

- Once the CDR adjunct has successfully retrieved a data file from the server and verified that it contains valid data, the adjunct deletes the data file from the server.
- The server automatically removes any CDR data file stored on its local hard drive that is older than 5 days.
- The onsite or remote switch administrator/technician (with proper permissions) deletes unwanted CDR data files.

CDR administration

Each Session Manager can have CDR either disabled or enabled.

Passwords are set up for each Session Manager which has CDR enabled. The Session Manager administrator creates a password for the designated use CDR_User. These need to be provided to the CDR adjunct administrator so that the adjunct can retrieve the CDR data files. The administrator should verify that this login and password work on each server on which CDR is administered.

CDR can be set when adding a new instance. If CDR has not been enabled and you wish to enable it:

1. Edit the Session Manager instance:
   a. On the System Manager Common Console, select **Session Manager**.
   b. Select the Session Manager instance and click on the **Edit** button.

   c. In the CDR section at the bottom of the screen, check the **Enable CDR** box, enter a password, re-enter the password to confirm it, and click on **Save.**

2. Edit the SIP Entity(ies):

   a. On the System Manager console, select **Network Routing Policy > SIP Entities**.

   b. Select the appropriate SIP Entity and click the **Edit** button.

   c. in the **Call Detail Recording** field, there are four choices in the drop-down menu (ingress, egress, both, none). The default is egress for SIP entities of type SIP Trunk. The default for all other types is none. Select the appropriate choice and click on **Commit.**

Administration notes

If at least one of two entities has CDR enabled, then CDR records will be created.

In route-through scenarios where one Session Manager routes directly to another Session Manager, CDR is recording only on the originating Session Manager if so administered, not the terminating Session Manager.

For more information regarding Session Manager CDR, contact your Avaya representative.

CDR alarms

Alarms are generated when CDR detects problems with recording. These alarms mean that if CDR was enabled for calls to or from certain SIP entities, call accounting for those calls is not available. During the outage, some or all calls will not be recorded in CDR.

Alarms need to be cleared manually by the administrator or maintenance support when the failure condition has been resolved.

The following is an example of alarm text:

- There is a problem with the Call Detail Recording (CDR) system. Call accounting is not operational

The following is an example of text when the alarm clears:

- Call Detail Recording (CDR) system is now operational. Call accounting is resumed

See CDR Not Operational for more information. If the problem continues or the alarm does not go away, contact your Avaya Technical Support.

Chapter 6: Maintenance functions

The following maintenance functions are available:

- Backup and restore
- Shut down/reboot the server

Backup and restore

The backup and restore functions are executed on the System Manager.

All of the configuration data that is needed to run the entire system, the System Manager, and all the Session Manager Instances is kept centrally on the System Manager. This means one backup contains all the data for the entire system. Individual backups of the Session Managers are not needed.

After a restore, the restored configuration data is automatically propagated down to the Session Managers.

Backing up System Manager

To backup files on a System Manager:

1. Select **Settings > Backup and Restore** in the left navigation pane on the System Manager Common Console.
2. Click **Backup** to start backing up data on the System Manager.

Restoring System Manager

To restore files:

1. Select **Settings > Backup and Restore** in the left navigation pane on the System Manager Common Console.
2. Click **Restore** to restore the backed up data.

The restore function restores the configuration files in the correct Session Manager instances.

Shut down/reboot the server

Starting with Service Pack 1, the Session Manager host server can be powered down safely and remotely if needed for hardware servicing. The shutdown/reboot feature also provides a safer last-chance restart instead of pressing the power button if the system becomes unresponsive. This feature is available for root, craft, and cust users.

If the Session Manager is shut down, on-site personnel will be required to restart the system.

There are two ways to shutdown or reboot the system:

- GUI procedure
- Command line interface

GUI procedure

The shutdown and reboot procedures are performed on the System Manager:

1. On the System Manager Common Console, select **Session Manager > Service State Administration**.
2. Select the Session Manager which needs to be shutdown or rebooted. Only one Session Manager can be shutdown or rebooted at a time.
3. Change the state of the Session Manager to **Deny New Service**. Wait for all active calls to end before shutting down or rebooting the server.
4. Click on the **Shutdown System** button.
5. Select **Shutdown** or **Reboot** from the drop-down menu. A confirmation screen will be displayed. If the Session Manager is not in the **Deny New Service** state, an additional screen with the recommended action will be displayed.

   Note:

   It is ***strongly*** suggested that the Session Manager be in the **Deny New Service** state and that you wait for all active calls to end before shutting down/rebooting the server. Active calls through the affected Session Manager will drop if it remains down too long. New calls will immediately use an alternate Session Manager (if available) once the affected Session Manager is placed in the **Deny New Service** state.

Command line interface

If you have problems accessing System Manager, use the command line interface with the following procedure:

1. Login as *cust* using a laptop.
2. Enter one of the following commands:
   - **`shutdownSM`** (to shut down the server)
   - **`rebootSM`** (to reboot the server)
3. If the Session Manager has been shut down, the confirmation screen will warn that on-site personnel will be required to restart the system.

Chapter 7: Data Retention

While the configuration data is kept on the system forever, there are other types of data that accumulate and need to be purged from time to time to avoid filling up the disk. These types of data are:

- Logging Data
- Alarming Data
- Backup Data

Logging and alarming data

Logging and alarming data are handled by data retention policies. The number of days that this data is retained is specified by a value called the retention interval. Each day, any data that is older than the specified retention interval is purged from the system.

The Data Retention web page allows you to view and change the retention interval. To access this page, click **Settings > Data Retention** in the left navigation pane on the System Manager Common Console.

The web page displays a list of retention rules and buttons to manipulate the rules (edit, update, cancel, apply). One rule is named **LogPurgeRule**. It is used to set how long logging data files are retained. Another rule, **ClrdAlarmPurgeRule**, is used to set how long cleared alarm data files are retained. Each rule is managed in the same way:

- Click the circle next to the rule to be managed.
- Click on the edit button to change the retention interval.
- Enter the desired value under the data retention column and click the update button.

Each rule is applied automatically once a day to purge old data. However, the apply button can be used to immediately apply the rule. Click on the circle next to the rule and click the apply button.

Backup data

Backup data retention is controlled by a maximum number of files rather than by time. When a new backup is initiated and the maximum number has been reached, the oldest backup file is removed in order to make room for the new backup file.

To access the page to view and change the number of backup files that are retained:

- Click **Settings > Service Profile Management > System Manager 1.0 > IMSM Element Manager** in the left navigation pane on the System Manager Common Console.

The web page displays a list of data attributes. The attribute for controlling the maximum number of backup files is named **Maximum Backup Files**. To change it, click the edit button in the bottom right of the web page, enter the desired value, and click the commit button. The new value will take effect when the next backup is run.

Chapter 8: Security Module Status

The Security Module Status page allows you to view the status and configuration of the security module for each administered Session Manager and to perform certain actions on the security module.

You can view the status of the security module such as its IP address, default gateway, QoS priority, and certificate authority.

You can reset, synchronize the security module, or assign a certificate authority.

To access the Security Module Status page, click **Session Manager > Security Module Status** in the left navigation pane on the System Manager Common Console.

The following security module statistics are displayed for each Session Manager.:

Field	**Description**
Security Module Deployment	Status of the security module deployed for the Session Manager (up or down)
IP Address	IP address of the security module used for SIP traffic. This field should match the address administered on the SIP Entity form for the Session Manager instance.
Network Mask	Network Mask of the security module. This value should match the network mask administered on the Session Manager instance form.
Default Gateway	Default Gateway used by the security module. This value should match the default gateway administered on the Session Manager instance form.
Interface Name	The Ethernet interface used by the security module for SIP traffic. This field is for informational purposes and is not administrable.
Name Server	DNS Servers used by the security module. This field is for informational purposes and is not administrable.
DNS Search	DNS search string used by the security module. This field is for informational purposes and is not administrable.
VLAN	The VLAN ID that the security module is associated with. This field should match the VLAN ID administered on the Session Manager instance form.
QOS	802.1q priority value (Layer 2 QoS) used by the security module. This field should match the QOS priority administered on the Session Manager instance form.

Field	Description
Assigned Certificate (CA)	The identity certificate being used by the security module for establishing TLS sessions. It can be either of two values: l **SIP CA** - This is the issuer of the default certificate. l **System Manager CA** – This is the unique certificate issued to the Security Module during installation.
Trusted hosts (expected/actual)	l The *expected* value is the number of Trusted SIP Entities configured in Network Routing Policy which have Entity Links to the Session Manager. l The *actual* value is the number of Trusted SIP Entities currently configured on the security module. l If these values do not match, then the Synchronize action should be performed (see below).

The Refresh button refreshes the display for all of the administered Session Manager instances. **Note**: This page does not automatically refresh.

The following actions can be performed on a selected Session Manager:

- Reset – Performs a reset the security module for the selected Session Manager. An administrator may choose to reset the security module when a connection cannot be made to the security module.

  Warning: The Session Manager cannot process calls while the security module is being reset. In a multiple Session Manager installation, refer to **System State Administration** for details on how to disable the Session Manager prior to resetting the security module.

- Synchronize – Performs an on-demand audit to verify that the administered configuration matches the actual configuration stored on the security module. This action should be performed anytime the values in the security module statistics table do not match the administered data.
- Security Module Certificate - Session Manager provides the capability of switching the active certificate being used by the security module to the default certificate or the unique certificate issued for that instance by the System Manager CA. Please refer to *Installing and Administering Avaya Aura*^{TM} *Session Manager, 03-603324* for more details about this operation. Additionally refer to the Session Manager Security Guide to understand the implications of doing this operation.

Possible causes for a “Down” Security Module Deployment status:

- The security module has recently been reset. A reset can take several minutes to complete. Use the refresh button to get the latest status.
- The security module has yet to receive its configuration from System Manager. Perform a synchronize action to trigger an update.
- There is a problem with security module that needs attention. Perform a reset of the security module.

Chapter 9: Data Replication Status

The Session Manager Data Replication Status page monitors the status of replication from the System Manager database (master) to the Session Manager local databases (replicas). Database changes on the master database are continuously monitored and sent to the replicas within seconds of being committed on the master.

The Data Replication system is robust and will repair itself via automatic connection recovery and replication audits. Replication audits keep the master (System Manager) and the replica databases (Session Manager instances) synchronized if connection problems occur, if database resource problems occur, or after a system has been down for upgrading, restore or recovery. The audit mechanism is a reliable incremental recovery mechanism to minimize the need for complete recovery from the master database.

To access the Security Module Status page, click **Session Manager > Data Replication Status** in the left navigation pane on the System Manager Common Console.

Field	**Description**
Records Currently in Database	Total number of records in each databases. The number of records in each replica database should match the number in the System Manager database because the data is replicated from the master database to the replica databases. There will be a slight difference during replication activity.
Records Pending Update	For the master database column, this means that the database modifications (insert/update/delete) have occurred on the master database, but update messages for these modifications have not yet been sent to the replica databases. For the replica databases, this means that a replica database audit has determined that these records need to be updated in this replica database, but this replica database has not yet received and processed the associated messages from the master database to perform these modifications.
Modification	Total number of database modifications (insert/update/delete operations) that have occurred in the respective databases.
Modifications Resulting from Audits	For the master database column, these are the number of database modifications that were sent as update messages to any of the replica databases in response to a replica audit. For the replica databases, these are the replica database modifications that were performed as a result of a database audit. This means that a replica audit determined the database was out of synchronization with the master database and requested and received updates from the master database.

Field	Description
Failed Modifications (replica only)	Number of database operations that have failed to be committed (insert, update, delete operations). This could be an error or it could be because the replication messages sent from the master to a replica database were received out of order, in which case, the failure will automatically recover.
Failed Modifications Resulting from Audit (replica only)	Number of database operations that have failed to be committed (insert, update, delete operations) only for those modifications that were executed as a result of a replica database audit.
Elapsed Time Since Last Update/Audit (Days H:M:S)	On the master database, this is the elapsed time since the last time audit requests were received or responded to. On the replica databases, this is the elapsed time since the last replica database audit was performed. On replicas the audit process is performed every 15 minutes.
Elapsed Time Since Last Update/Audit Requiring Modifications (Days H:M:S)	Same as above except that an audit found a database out of sync and updates where made to the replica database.
Last JMS Message Received (master) / Sent (replica)	This allows comparison of the last message received by the master to be compared to replica message send times. Typically no more then a couple of seconds or less difference appears when replication links are healthy. If there is a difference of more then a few seconds between any of the send times and the master receive time then a connection problem is indicated.
JMS Connection Status	This is the status of the underlying message transport system used by the data replication system. An OK status means that the message transport system works as intended. Any other status implies that there could be a problem sending messages from the master to the replica and from the replica to the master.
Test String Value	Current value of the test string in the master database. For the replica columns, this is the value of the test string in the respective database and should eventually match the master database test string value.
Test String Last Update Time	Time the test string was written to the database. This is an additional confirmation of the replication test success.

The Refresh button refreshes the display for System Manager and all of the administered Session Manager instances.

The following action can be performed on System Manager:

- Update on Master - Updates the Test String Value in the System Manager database so that you can verify that the test string is replicated to each Session Manager database. Enter any desired string, press the Update on Master Button, then wait a few seconds and press the Refresh button. The Test String Value and Last Update Time should match across all columns within a Refresh or two.

The following action can be performed on the System Manager and all Session Managers:

- Reset Modification Counters (All) - Resets the modification counters for the System Manager as well as all the administered Session Managers to zero. This can be used in combination with below on demand audits to isolate replication problems to the System Manager or a particular Session Manager.

The following action can be performed on selected System Manager or Session Managers:

- Start Audit/Update (Selected) – Start an update of the master database or starts an audit of the replica database on selected hosts.

When running an audit:

- If you select a Session Manager, this triggers an update cycle on the master database. This means that the System Manager replication looks for any modifications made to the master database and then sends updates to the replica databases if necessary. This process happens automatically every few seconds. So it is typically not necessary to do this on demand.
- If you select a Session Manager, this triggers a replica database audit. If the audit determines the replica database is out of sync with the master database, it will request updates from the master database. It may take more then one audit cycle to get the database in sync. This can occur due to the amount of data to be synchronized and/or if there are complex relationships between the data to be synchronized.

Chapter 10: Maintenance tests

The Maintenance Tests page allows you to perform functionality tests on the System Manager server and the administered Session Manager instances. These tests include testing the functionality of data replication and network connectivity to Session Manager instances, database functionality, and the security module of each Session Manager. The tests are run periodically by the system to monitor the health of system components. The same tests can also be executed on demand.

Tests are not run for a Session Manager if its state is set to **Management Disabled**.

Tests may fail if the server is down or not responding.

Running maintenance tests

The Maintenance Tests page allows you to run maintenance tests on the System Manager or any administered Session Manager in the enterprise.

1. From the System Manager Common Console navigation pane, select **Session Manager > Maintenance Tests**.
2. Select System Manager or a Session Manager instance to test from the pull-down list.
3. To run all the tests on the selected System or Session Manager, click **Execute All Tests**. To perform selected tests, select the tests from the list and click **Execute Selected Tests**.

Test network connections to each Session Manager

This test only runs on the System Manager. It tests the connectivity to each currently administered Session Manager.

If connectivity is up for each Session Manager, the test passes. Otherwise, the test fails. The server could be down or an upgrade/install is in progress. Check the log, then check Log and Alarm Event IDs for the appropriate troubleshooting action.

Test data replication to each Session Manager local database

This test only runs on the System Manager. It tests if replication is functioning properly to each currently administered Session Manager. A test string is sent to each administered Session Manager. The test string is saved by each Session Manager within its respective database. After a short wait, each Session Manager is queried for the test string value.

The test is not run for a Session Manager if there is a JBoss connection problem or the current state of the Session Manager is set to **Management Disabled**.

If the replication succeeds, the test passes. A failure indicates a possible JMS or secure connection problem. Refer to the Data Replication Status page for more information.

A similar test can be executed on-demand on the Data Replication Status page. In that case, you can specify a custom test string.

Test Call Processing status

This is a call processing sanity test. If call processing is working properly, the test passes. If the test fails, contact Avaya Technical Support.

Test Service Host status

Tests the status of the Service Hosts. This test asks for a list of service hosts and determines the running (up/down) status of each. The test fails if one or more of the hosts has an invalid status. Otherwise, the test passes. If the test fails, contact Avaya Technical Support.

Test Service Director Status

This tests the status of the SIP A/S Service Director using a connection to SIP A/S. The test passes if the status of the service director is valid. If the test fails, contact Avaya Technical Support.

Test SIP A/S Management Server Status

This tests the status of the SIP A/S Management Server using a connection to SIP A/S. The test passes if the status of the management server is valid or a particular SIP A/S service is running.

If the test fails, contact Avaya Technical Support.

Test sanity of Secure Access Link (SAL) agent

This test can run on either System Manager or Session Manager. It checks if the Security Access Link agent is running or not on the server. If the link is up and running, the test passes. Otherwise, if the test fails, contact Avaya Technical Support.

Test management link functionality

Test the administrative link to Session Manager. If this test fails, administrative changes will not take effect on Session Manager. Otherwise, the test passes.

Test Security Module Status

Queries the basic status of the SM100 Security Module. If the query is successful, the test passes. Otherwise, it fails.

Test Postgres database sanity

This test runs on either System Manager or Session Manager. System Manager tests the sanity of the master database. Session Manager tests the sanity of its local instance database. A replication test from System Manager indirectly checks the sanity of each Session Manager replica database.The test passes if the test is successful. If the test fails, contact Avaya Technical Support.

Chapter 11: SIP Monitoring

SIP Monitoring provides background detection for monitored connections to improve alternative routing and minimize the call setup time due to SIP link failures.

The SIP entity being monitored should support the SIP OPTIONS method in order to be monitored.

SIP Monitoring can only report problems if the SM100 Security Module is functional.

The SIP Monitor periodically tests the status of the SIP proxy servers. If a proxy fails to reply, SIP messages are no longer routed to that proxy. As a result, call delays will be reduced since calls will not be routed to the failed servers.

The SIP Monitor will continue to monitor the failed SIP entity. When the proxy replies, SIP messages will again be routed over that link.

You can turn monitoring on or off for a given SIP entity. If monitoring is turned off, the SIP entity will not be monitored by any instance.

You can also turn monitoring on or off for an entire instance. If monitoring is turned off, none of the SIP entities will be monitored by this instance. If monitoring for the instance is turned on, only those SIP entities for which monitoring is turned on will be monitored.

SIP Monitoring setup is administered through the Network Routing Policy screens on the System Manager.

SIP Monitoring web page

To access the SIP Entity Link Monitoring Status Summary page, click **Session Manager > SIP Monitoring** in the left navigation pane on the System Manager Common Console.

The SIP Entity Link Monitoring Status Summary page displays the status of the entity links for all administered Session Manager instances. An entity link consists of one or more physical connections between a Session Manager and a SIP entity. If all of these connections are up, then the entity link status is “up”. If one or more connections are down, but there is at least one connection up, then the link status is “partially down”. If all of the connections are down, the entity link status is “down”.

Chapter 12: Tracing

SIP Tracer allows advanced tracing of SIP messages exchanged between the Session Manager server and remote SIP entities. SIP Tracer consists of two components:

- Tracer Configuration - defines the characteristics of messages to be traced for the capturing engine in the Security Module
- Trace Viewer displays the captured SIP messages

You can use SIP message tracing to troubleshoot or monitor a selected Session Manager instance. SIP tracing enables the logging of incoming and outgoing SIP messages in the SM100 framework. SIP messages that are dropped by any of the SM100 components such as SIP firewall are also logged by the SIP tracer. You can trace all the messages belonging to a user for a call or for a selected Session Manager instance.

Tracer Configuration

The Tracer Configuration page allows you to configure tracing properties for each administered Session Manager. The output of the SIP Trace is viewable on the System Manager.

There are three Call Filters and three User Filters which can be configured separately for each Session Manager in the cluster. Each time a new Tracer configuration is sent to a Session Manager, the existing Tracer configuration is overwritten.

The Tracer Configuration page has four sections:

1. Basic configuration: This section has six check boxes that control the basic functionality of SIP Message tracer:

Check Box	Description
Enabled	Enable/disable SIP message tracing.
Dropped	Enable/disable tracing of dropped SIP messages by the Security Module.
From Network to Security Module	SIP message tracing for calls sent to the Session Manager instance from the network.
From Security Module to Network	SIP message tracing for calls originating from the Session Manager instance and sent to the network.

Check Box	Description
From Server to Security Module	Traces internal SIP messages originating from the Session Manager SIP server to the Security Module.
From Security Module to Server	Traces internal SIP messages originating from the Security Module to the Session Manager SIP server.

2. User Filter: To filter SIP messages based on the users, click **New** under **User Filter**. You can define a maximum of three separate user filters. An empty value in the From and To fields means that every message matches. The format for a valid sender/receiver is sip:1234@xyz.com, where 1234 is the user and xyz.com is the domain.

   To delete an existing user filter, check the box next to the filter and click **Delete**.

Field	Description
From	Trace SIP messages which match the sender in the "from" SIP header. Enter sender information.
To	Trace SIP messages which match the receiver in the "to" SIP header. Enter receiver information.
Max Message Count	Enter a value for the maximum number of messages matching the filter which Session Manager should trace. The default value is 25

3. Call Filter: To filter all SIP messages that start a new call, click **New** under **Call Filter**.

   You can define a maximum of three separate call filters.

   All the messages in a call are identified by their unique call ID, To tag, and From tag from the header values.

   A valid sender/receiver string, for example, is: sip:1234@xyz.com, where 1234 is the user and xyz.com is the domain.

   An empty value in the From and To fields means that eve message matches.

   To delete an existing call filter, select the filter and click **Delete**.

Field	Description
From	Trace SIP messages which match the sender in the "from" SIP header
To	Trace SIP messages which match the receiver in the "to" SIP header
Max Call Count	Enter a value for the maximum number of messages matching the filter which Session Manager should trace. The default value is 25
Request URI	Trace SIP messages which match the receiver in the SIP Request-uri header. A valid Request URI format is .@192.111.11.111

4. Session Manager Network: Select one or more of the administered Session Manager instances from the list under Session Manager Network on which to apply the filters.
5. Click the **Commit** button to apply the filters to the selected Session Managers. Any previous filter configurations are overwritten.

To configure SIP tracing, select **Session Manager** > **Tracer Configuration** in the left navigation pane of the System Manager Common Console.

Trace Viewer

Trace Viewer allows you to view SIP message trace logs based on the filters that you have configured. You can view these trace logs for a range of hours or days and for selected Session Manager instances.

To view the trace logs:

1. Select **Session Manager > Trace Viewer** in the left navigation pane of the System Manager Common Console.
2. To filter trace logs for a range of hours or days, enter or select the date, time, and time zone information under the From and To areas. This filter criteria will display only those logs with a time stamp between the From and To values.
3. Select one or more Session Manager instances for which you wish to see the trace logs.
4. Click **Commit** to generate the trace output.

   The output displays trace logs with the following information:

   - Details–Click on **Show** to see the complete message.
   - Time–time at which the trace record was written
   - Tracing Entity– Name of the Session Manager which logged the trace
   - From–URI from where the traced SIP message originated
   - Action - The Request/Response Action of the traced SIP message (e.g., INVITE, ACK). An arrow indicates the direction of the action (e.g., --INVITE->, <-By--).
   - To–URI to which the traced SIP message was sent
   - Protocol–Protocol that was used by the traced SIP message such as TCP, UDP, TLS
   - Call ID–Call ID of the traced SIP message

The following operations can be performed on the Trace Viewer page:

- Dialog filter - this button is enabled if at least one table entry is selected. Trace messages are displayed which are related to the same dialog.
- Cancel - this button is enabled if a Dialog Filter is active. Selecting this button will cancel the Dialog Filter and the original Trace Viewer page is displayed.

- Hide/Show dropped message - This is a toggle button. "Hide dropped messages" will not display any dropped messages, thereby reducing the number of messages displayed. "Show dropped messages" will display all messages.

Hints:

- "Records retrieved" versus displayed items:

  Within the left corner of the Trace Viewer page, the number of listed trace messages is displayed. Due to system performance, not all trace messages which match the filter criteria may be displayed. In this case, the value of "Records retrieved" will be greater than the displayed Items value. It is suggested that the filter criteria be changed to ensure that no relevant trace messages are missing within the Trace Viewer list.
- Due to the Trace Configuration filter options, trace records may be shown multiple times.

Exporting Trace Viewer files

Starting with Service Pack 1, you can capture a SIP tracing view to a file. The Trace Viewer screen displays a **More Actions** button which is active only if one or more trace records are listed. The retrieved Trace Viewer list can be saved to a file on the client side. The **Hide/Show dropped messages** and **Dialog Filter** functions are operational for the exported file but the GUI filters and sorting operations are not.

There are two options under the **More Actions** drop-down menu:

- Export Trace Viewer Overview
- Export Trace Viewer Details

For the Trace Viewer Overview file, a tab-separated plain text file is created with all of the overview columns which appear on the Trace Viewer screen. The file can be displayed with a text editor such as Wordpad or a tabulator editor such as Excel.

For the Trace Viewer Details file, a plain text file is created with the details of the Trace Viewer records.

When you select one of the export options, you can:

- Open the Trace Viewer list with an editor
- Save the Trace Viewer list to a file
- Perform the open or save function automatically for files from now on. This option appears if you are using Mozilla Firefox as your browser. If you are using Internet Explorer, this option does not appear.

Chapter 13: Call Routing Test

The Call Routing Test provides verification of System Manager administration for routing a **Calling Party URI** to a **Called Party URI**.

Use it to verify that you have administered the system as intended before placing it into service or to get feedback on why a certain type of call is not being routed as expected. No real SIP messages are sent during this test.

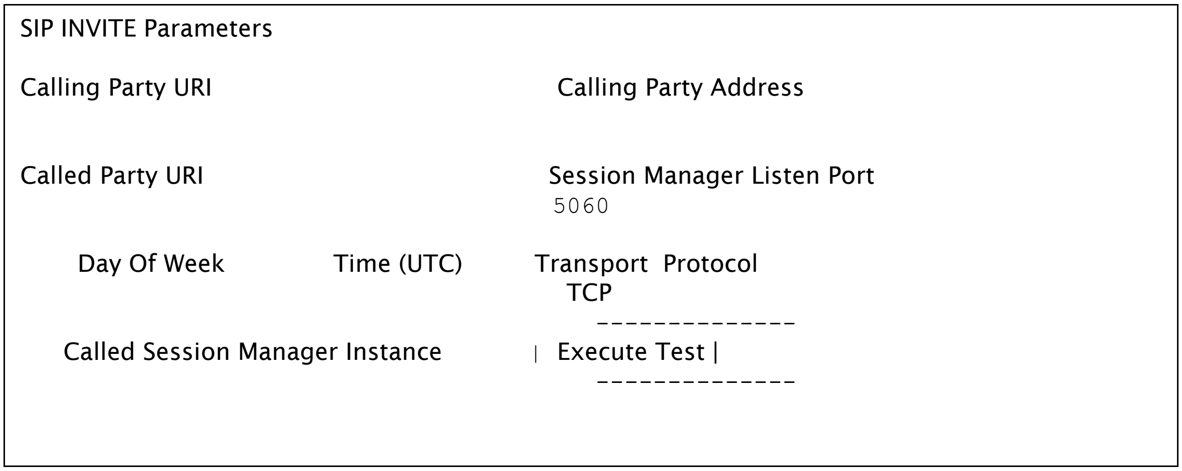
This test displays the routing decision process as it uses the SIP routing algorithms. It uses administration from the following forms:

- **Network routing Policy > Adaptations, Dial Patterns, Entity Links, Locations, Routing Policies, SIP Domains, SIP Entities, Time Ranges**
- **Session Manager > Session Manager Administration**

Call Routing Test setup

The following steps explain how set up the call routing test for a Session Manager:

1. Click on **Session Manager > Call Routing Test** in the left navigation pane on the System Manager Common Console.
2. Enter information for a SIP INVITE message for both **Calling** and **Called Party URIs** and click **Execute Test.**



SIP INVITE Parameters

Calling Party URI Calling Party Address

Called Party URI Session Manager Listen Port
5060

Day Of Week Time (UTC) Transport Protocol
TCP

Called Session Manager Instance | Execute Test |

The fields and their descriptions are:

Field Name	Example/Description
Called Party URI	Use this format: **sip:12345@MyOtherCompany.com** The leading digits (*12345)* are from the **Dial Pattern** page. The domain - *MyOtherCompany.com* - is the **SIP Domain** associated with the *Called Party'*s Session Manager Instance.
Calling Party Address	**192.168.0.1** - Enter the IP address of the **SIP Entity** that the *Calling Party* is associated with. For CM, it could be a *procr* or a *CLAN.*
Calling Party URI	Use this format: **sip:67890@MyCompany.com** The leading digits (*67890* are from the **Dial Pattern** page. The domain - *MyCompany.com* - is the **SIP Domain** associated with the *Calling Party'*s Session Manager Instance.
Session Manager Listen Port	Enter the Listen port number which is administered on the **Entity Links** form which the *Calling Party* is associated with.
Day of Week	From the drop-down menu, select a day of the week. This entry uses the **Time Ranges** associated with the *Calling Party's* **Routing Policy.**
Time (UTC)	Enter a time, or use the default which is the current time. This entry uses the **Time Ranges** associated with the *Calling Party's* **Routing Policy.**
Transport Protocol	From the drop-down menu, select a Transport Protocol. The selected Protocol must be one which is administered on the **Entity Links** form which the *Calling Party* is associated with.
Called Session Manager Instance	From the drop-down menu, select the Session Manager Instance that the Calling party will use for this test call.

After clicking **Execute Test**, two headings with information about the test are displayed: **Routing Decisions** and **Routing Decision Process**

Test Results

The “Routing Decisions” output will contain one line per destination choice (there will be more than one line if there are alternate routing choices and the lines will be in the order that destinations would be attempted). Note that each line tells you not only where the INVITE would be routed, but also what the adapted digits and domain would be.

The “Routing Decision Process” contains details about how the Routing Decisions were made.

No Data Returned

The test failed.

Routing Decisions - will display *No data to display*

Routing Decisions Process - will display *Unable to resolve <IP Address for Calling Party Address> to a recognized entity*

This message indicates that System Manager could not successfully route the call using all of the information entered to execute the test. Verify that all of the information is entered according to the exact format as listed in the table above. If the test still fails, verify all administration associated with the *Calling Party* and *Called Party URIs.*

Data Returned

The test passes.

Routing Decisions - will display data similar to the following:

```
< sip:12345@MyOtherCompany.com > to SIP Entity ’CalledPArtySIPentity’
port ’MyPortNumber’ using TCP/TLS/UDP.
```

Note: calls with multiple possible destinations will display multiple rows, and route-through scenarios will include route-through information.

Routing Decisions Process - will display data similar to the following:

```
NRP Sip entities: Originating SIP Entity is "SIP Entity Name"

Using digits < 12345 > and host < MyOtherCompany.com > for routing.

NRP Dial Patterns: No matches for digits < 12345 > and domain <
MyOtherCompany.com >

NRP Dial Patterns: No matches for digits < 12345 > and domain < null >

NRP Dial Patterns: No matches found for the originator’s location.
Trying again using NRP Dial Patterns that specify -ALL- locations.

NRP Dial Patterns: No matches for digits < 12345 > and domain <
MyOtherCompany.com >

NRP Dial Patterns: Found a Dial Pattern match for digits < 12345 > and
domain < null >.

Ranked destination NRP Sip Entities: ’CalledPartySIPentity’

Removing disabled routes.

Ranked destination NRP Sip Entities: ’CalledPartySIPentity’

Adapting and proxying to SIP Entity ’CalledPartySIPentity’

NRP Adaptations: Doing ingress adaptation.

NRP Adaptations: Changed P-Asserted-Identity header to
sip:67890@MyCompany.com as part of adaptation.

NRP Adaptations: Doing egress adaptation.

Routing < sip: 12345 @ MyCompany.com > to SIP entity
’CalledPartySIPentity’ port ’MyportNumber’ using TCP/TLS/UDP.
```

Chapter 14: Replacing Hardware

This section describes how to replace the field replaceable units (FRUs) for a Session Manager.

The following hardware components can be replaced:

- Avaya S8510 Server
- Hard Drives
- SM100 Card
- Power Supplies
- Memory Modules

Replacing the Avaya S8510 Server

For Session Manager Release 1.1, only services personnel will be able to replace the server since root permission is required for shutting down and rebooting the server.

Replacing a hard disk drive

The Hard Disk Drive is monitored by capability built into the hard disk drive unit. Some hard disk drive problems do not occur suddenly. They are a result of a gradual degradation of components over time.

The hard drives are mirrored for speed and reliability and are hot-swappable (you do not need to power down the server to replace either drive). However, you cannot remove both drives at the same time.

Also, do NOT remove the healthy, active hard drive. If you inadvertently remove the active hard drive, you ***cannot*** plug it back in. If the active hard drive is removed, you must:

- Cleanly power down the server at an appropriate time.
- Re-insert the active hard drive in its original slot.
- If the bad drive is still installed, remove the drive from the slot, and set it aside.
- Power-up the server with only the healthy drive present. Make sure the server comes up and is operating normally.
- Proceed with Replacing the defective hard drive.

Replacing the defective hard drive

The hard drive replacement procedure can destroy data stored on the hard drive. *Before* replacing either hard drive, perform a server data backup first. This is the first step in the procedure.

Tools required:

- S8510 Hard Disk Drive replacement
- Electrostatic wrist ground strap and mat
- Key to server keylock on front bezel

To replace a defective hard drive:

1. Backup data on the Session Manager server:
    a. Select **Settings > Backup and Restore** in the left navigation pane on the System Manager Common Console.
    b. Click **Backup** to start backing up data on the System Manager.
2. While wearing an antistatic wrist ground strap, remove the front bezel and cover to access the hard drives.
3. Identify the defective hard drive by checking the LEDs on the hard drives. The following table describes the meaning of the LED colors and patterns.

Drive status LED	Description
Off	Drive is ready for insertion or removal
Flashes green, amber, off	Drive is failing
Flashes amber four times per second	Drive has failed
Flashes green slowly	Drive is rebuilding
Steady green	Drive is online
Flashes green 3 seconds, amber 3 seconds, off 6 seconds	The rebuild aborted

4. Remove the defective drive:
    a. Pinch together the two tabs of the drive carrier release handle.
    b. Open the carrier release handle. Wait about 10 seconds to allow the internal mechanism to park the read/write heads so that the drive can be handled safely.
    c. Pull the hard drive out of the slot.
    d. Set the hard drive on an antistatic mat.

5. Insert the replacement hard drive in the slot and push until it is seated.
6. Close the hard drive carrier handle to lock the hard drive in place.
7. Replace the front bezel and cover.
8. The RAID software rebuilds the hard drive automatically in approximately 80 minutes, during which time the hard drive LED flashes green slowly.
9. Return the defective hard drive.

Replacing the SM100 Card on the Avaya S8510 Server

Required tools:

- Replacement SM100 card
- #2 Phillips (cross-point) screwdriver
- Electrostatic wrist ground strap and mat
- Key to front bezel

SM100 Card replacement procedure

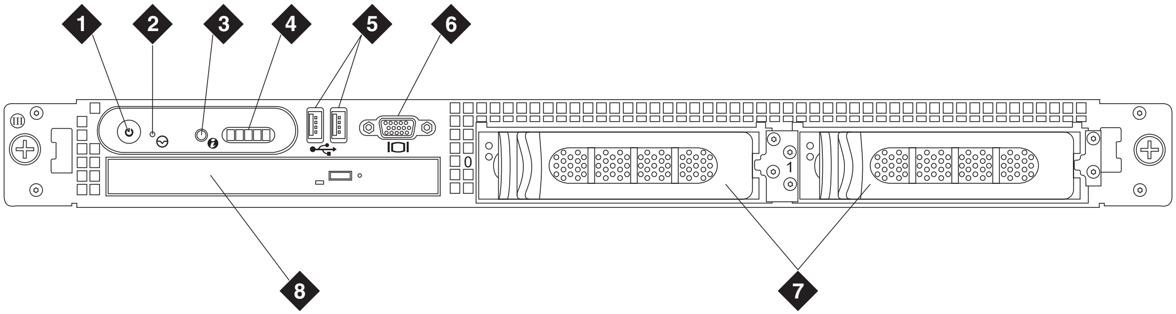
The steps to replace an existing SM100 Security Module with a new SM100 card are:

1. Power down the server
2. Label and disconnect cabling
3. Remove the S8510 server from the rack
4. Remove the cover of the S8510 server
5. Remove the defective SM100 card
6. Install the replacement SM100 card in the S8510 server
7. Replace the cover on the S8510 server
8. Install the S8510 server in the rack
9. Return the defective equipment

Power down the server

Power down the S8510 server by pressing the power button on the front panel. Wait until the server has been powered down and the power-on indicator light is off. (Note 1 in the following figure).

Figure 2: Avaya S8510 Front Panel



hw8510fn LAO 020108

Figure notes:

1. Power-on indicator, power button
2. Nonmaskable Interrupt (NMI) button (disabled)
3. System identification button (used to locate equipment within the rack)
4. LCD display (system ID, status information, and system error messages)
5. USB 2.0 connectors
6. Video connector (not used)
7. Hard disk drives
8. Slimline CD/DVD drive

Label and disconnect cabling

Label and disconnect the following connections:

- Label and disconnect the power cords from the power supplies at the back of the server.
- Label and disconnect the LAN connection from the Ethernet port on the SM100 at the back of the server.

Remove the S8510 server from the rack

CAUTION:

Ensure that power is completely removed from the server. *Power cords must be detached from the power supplies.*

To remove the S8510 server from the rack:

1. Ensure that all cables are labeled and disconnected from the server.
2. Loosen the captive screws on both sides of the server (Note 1 in Figure 3).
3. Slide the server clear of the rails (Note 2 in Figure 3).

4. Release the rail lock by pushing the level in as you slide the server out of the rack (Note 3 in Figure 3).

Figure 3: Remove the S8510 server from the rack

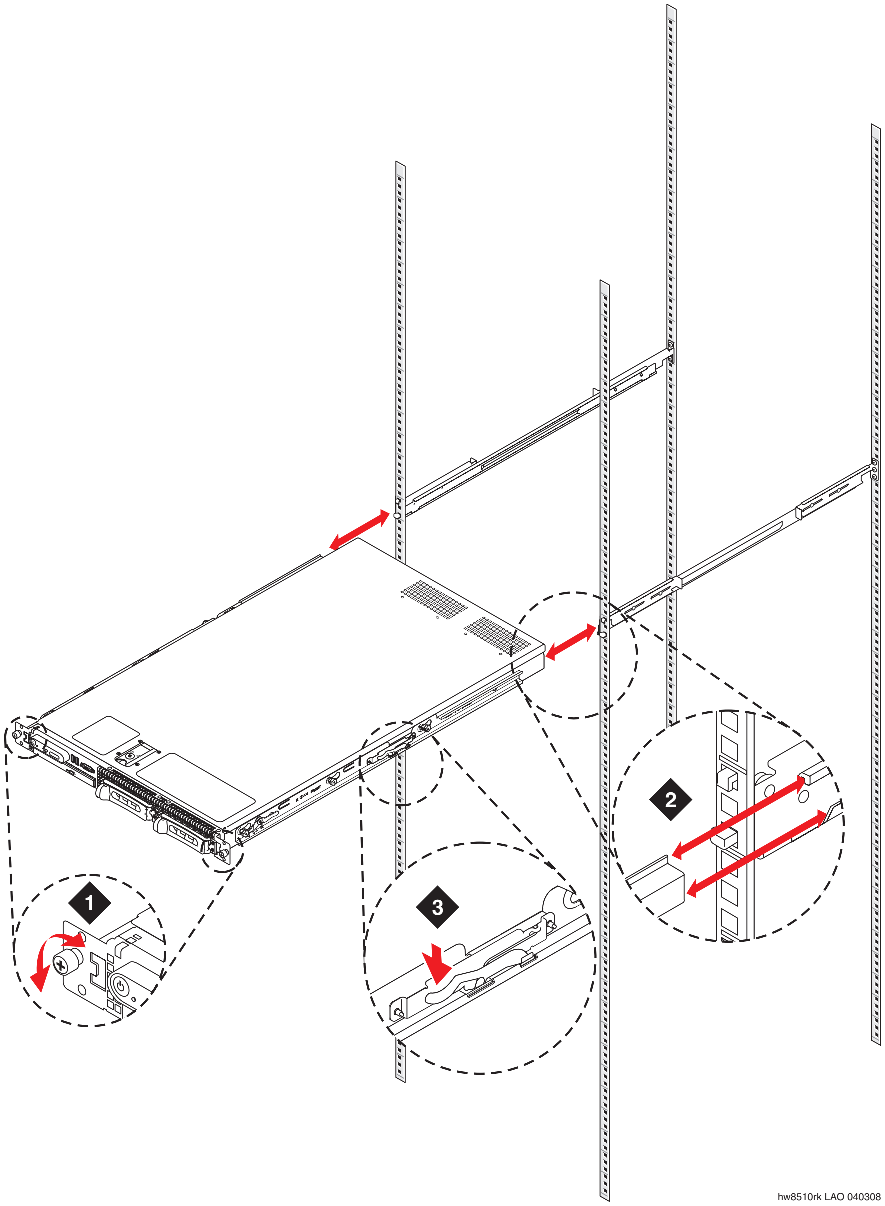


Figure notes:

1. Loosen the captive screws.
2. Slide the server clear of the rails.
3. Release the rail lock.

Remove the cover of the S8510 server

To remove the cover of the S8510 server:

1. Use a #2 Phillips (cross-point) screwdriver to rotate the latch release lock counter-clockwise to the unlocked position (Note 1 in Figure 4).
2. Lift the latch to unlock (Note 2 in Figure 4).
3. Lift the cover back, then straight up, and set it aside (Note 3 in Figure 4).

Figure 4: Removing the cover of the S8510 server

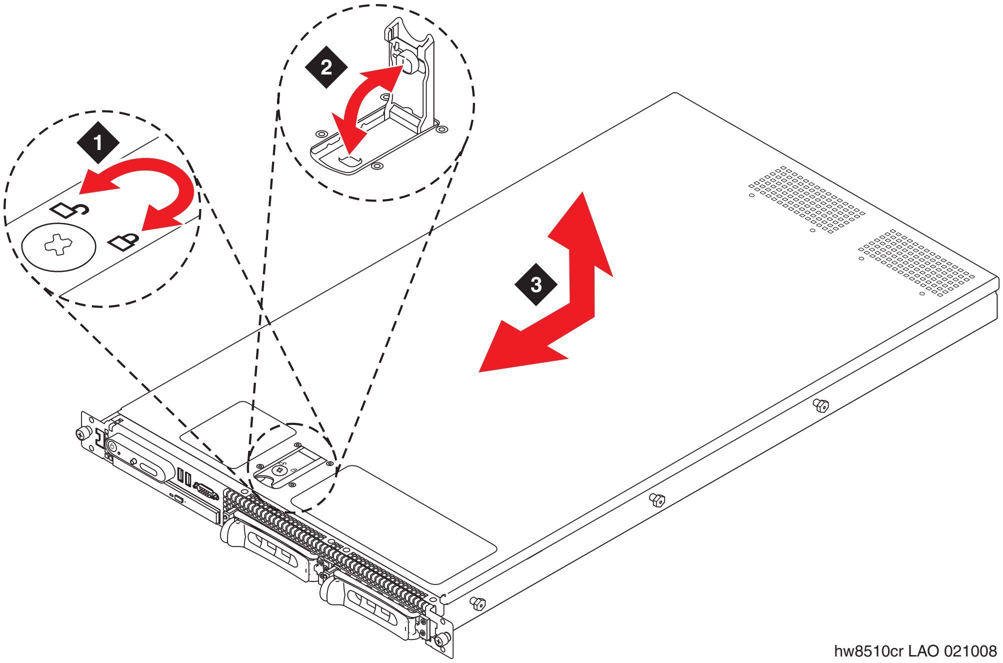


Figure notes:

1. Turn the latch release lock counter-clockwise to the unlocked position.
2. Lift the latch up to unlock.
3. Slide the cover back then lift straight up to remove.

Remove the defective SM100 card

ELECTROSTATIC ALERT:
Take precautions against electrostatic discharge. Wear a wrist strap connected to an approved ground.

The SM100 security module resides in a PCI expansion card rise at the rear of the S8510 server. To remove the defective SM100 from the riser:

1. Lift the release latches on the PCI expansion card riser (Note 1 in Figure 5).
2. Remove the defective SM100 card by pulling it gently out of the expansion slot in the rise assembly (Note 2 in Figure 5).

Figure 5: Removing/replacing the SM100 security module card

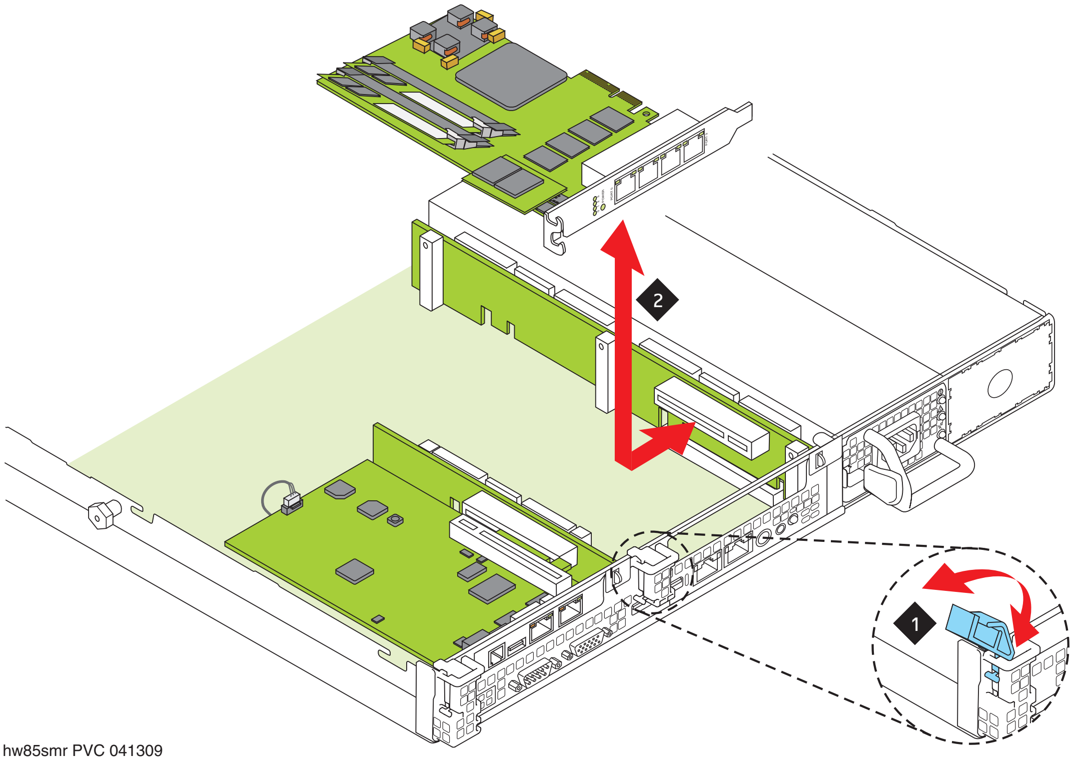


Figure notes:

1. Press the release latches on the PCI expansion card riser.

2. Remove the defective SM100 from the expansion slot.

Install the replacement SM100 card in the S8510 server

To install the replacement SM100 card in the S8510 server, refer to Figure 5: Removing/ replacing the SM100 security module card and perform the steps in reverse order:

1. Carefully grasp the replacement SM100 card by the outer edges and align it with the opening on the PCI expansion slot riser assembly. Press the SM100 firmly into the expansion slot (Note 2 in Figure 5). Make sure it is completely seated in the expansion slot.
2. Press the PCI expansion card riser release latches to secure the SM100 card and the riser assembly (Note 1 in Figure 5).

Replace the cover on the S8510 server

Refer to Figure 4: Removing the cover of the S8510 server and perform the steps in reverse order. Ensure that any internal cables are clear of the cover before replacing it on the server.

1. Place the cover on top of the server, aligning it with the J hooks on the sides (Note 4 in Figure 4).
2. Slide the cover forward (Note 3 in Figure 4).
3. Push the latch down to lock (Note 2 in Figure 4).
4. Rotate the latch release lock clockwise to secure the cover (Note 1in Figure 4).

Install the S8510 server in the rack

To install the S8510 server back in its rack:

1. Install the server onto the side rails in the rack (see Figure 3: Remove the S8510 server from the rack)
2. Reconnect the Ethernet cable to the dual NIC at the back of the server.
3. Reconnect the LAN connection (if used) from the Ethernet port on the SM100 at the back of the server.
4. Reconnect the power cords to the power supply at the back of the server.
5. Push the server completely into the rack and secure into place with the two captive screws on both sides of the server
6. Power up the server by pressing the power button on the front of the server.

Return the defective equipment

To return the defective equipment:

1. Place the defective equipment in the protective packaging that accompanied the replacement part(s).
2. Return the defective equipment to Avaya using the procedures established for your region.

Replacing a power supply

The power supplies are hot-swappable. You do not need to power down the server.

Before replacing a power supply, check that the power cord is connected and plugged into a non-switched outlet. The problem may be the connection, not the power supply.

To reduce the risk of personal injury from hot surfaces, allow the power supply to cool before touching it.

To replace a defective power supply:

1. Open the cable management arm, if present, to access the rear panel.
2. Identify the defective power supply by looking for the power supply fault indicator (middle indicator on the power supply).
3. With your thumb, press the release (orange) tab and the black handle together and pull out the power supply. Set it aside.
4. Insert the new power supply into the slot.
5. Ensure that the tab is locked into place and the power supply is securely seated in the slot.
6. Connect the power cord to the power supply.
7. Route the power cord through the cable management arm or power cord anchor, if present.
8. Close the cable management arm, if present.
9. Connect the power cord to the power source.
10. Make sure that the power supply LED is green.
11. Return the defective power supply.

Replacing the memory

Required tools:

- Replacement memory module
- #2 Phillips (cross-point) screwdriver
- Electrostatic wrist ground strap and mat
- Key to front bezel

To replace the memory modules:

1. Power down the server
2. Label and disconnect cabling

3. Remove the S8510 server from the rack
4. Remove the cover of the S8510 server
5. Replace the memory modules:
   a. Remove the protective cover over the memory modules.
   b. Remove the defective pair of memory modules.
   c. Insert the new memory modules.
   d. Replace the protective memory module cover.
6. Replace the cover on the S8510 server
7. Install the S8510 server in the rack
8. Return the defective equipment

Chapter 15: Changing configuration information

The following sections explain how to change the IP address or server name of a Session Manager and the IP address of a System Manager. These attributes can be changed after the initial installation. The procedures do not affect service.

Session Manager: Changing IP Address or Server Name

The person performing the IP address change must have access to the craft login on the Session Manager that whose IP address is to be changed. The steps are as follows:

1. Log into System Manager and click on **Session Manager > System State Administration**
2. Select the appropriate Session Manager, click on the **Service State** button, and select Deny New Service.
3. Wait for the active call count for Session Manager to be acceptably low (ideally, zero).
4. If the server is to be relocated, power it down, relocate it, and power it up.
5. Log in to Session Manager using the services port and the craft login.
6. Run the SMnetSetup command, specifying the desired IP information. You may proceed to the next step before this step completes.
7. Log into System Manager and navigate to **Session Manager > Session Manager Administration.** Select the appropriate Session Manager instance, click on the **Edit** button, and change any necessary IP information.
8. To change the associated host name, navigate to **Network Routing Policy > SIP Entities** and change the associated host name or IP address as desired.
9. For all other SIP entities with links to the changed Session Manager, change the provisioning of these links using the entity's administration. For example, if An Avaya Communication Manager communicates with Session Manager, its signaling groups will need to be updated to connect to Session Manager at its new location.
10. Once all provisioning has been changed and the SMnetSetup script has completed, check System Manager's **Session Manager > Data Replication Status** page to make sure that replication to Session Manager is functioning.
11. Run the maintenance tests for Session Manager prior to putting it back in service:
    a. From the System Manager Common Console navigation pane, select **Session Manager > Maintenance Tests**.
    b. Select the Session Manager instance from the pull-down list and click **Execute All Tests**.

12. On System Manager, click on **Session Manager > System State Administration** and **Accept New Service** for Session Manager. Verify that traffic is going to Session Manager again.

Caveat: May need to reinitialize Trust Management

System Manager: Changing IP Address

The person performing the IP address change must have access to the craft login on each Session Manager and the root login on System Manager.

The steps to change the IP address on System Manager are:

1. Log into System manager and navigate to **Settings > Backup and Restore.** Execute a backup on the System Manager.
2. From System Manager, navigate to **Session Manager > System State Administration** and disable all Session Managers.
3. Move System Manager and change its IP address as desired. Ensure that /etc/hosts is updated as well as any DNS configuration.
4. Execute the /opt/Avaya/bin/IPchange script on System Manager, passing it the old and new IP addresses according to the usage statement.
5. Execute the /opt/Avaya/bin/changeManagementIP script on each Session Manager, specifying the new System Manager IP address.
6. Management Enable All Session Managers.
7. From System Manager, navigate to **Session Manager > System State Administration.** Management Enable all Session Managers.
8. Verify management connectivity using the Test String mechanism on the **Session Manager > Data Replication Status** page.

Caveat: May need to reinitialize Trust Management.

Chapter 16: Testing the installation

The following steps should be done in order to verify the successful installation and configuration of System Manager and Session Manager. These steps verify that the software is installed and configured properly, and that the servers and applications are communicating.

Before running the maintenance tests below, you need to have already added the Session Manager Instances into System Manager. This is done using the **Network Routing Policy > SIP Entities** and **Session Manager > Session Manager Administration** pages in the left navigation pane on the System Manager Common Console.

To verify the installation of System Manager and Session Manager:

1. Click **Session Manager > Maintenance Tests** in the left navigation pane. Select the System Manager server in the pull down list, and click on Execute All Tests. Verify all tests show Success status. If the data replication test fails, refer to the **Session Manager > Data Replication Status** page to identify which Session Manager is having replication problems.
2. Display SM100 board status by clicking **Session Manager > Security Module Status** in the left navigation pane. Verify that Security Module Deployment is Up for all Session Managers.
3. Click **Session Manager > System State Administration** in the left navigation pane. Verify the installed software versions of all Session Managers are the same version and that all Session Manager servers are in the Management Enabled state.
4. Click **Session Manager > Maintenance Tests** in the left navigation pane, select each Session Manager instance, and click on Execute All Tests. Verify all tests show Success status.

.

Chapter 17: Service Pack upgrades

For Session Manager Release 1.1, only service pack upgrades are available. The upgrade for Service Pack 1 requires root access. Contact your Avaya representative for the Service Pack 1 upgrade.

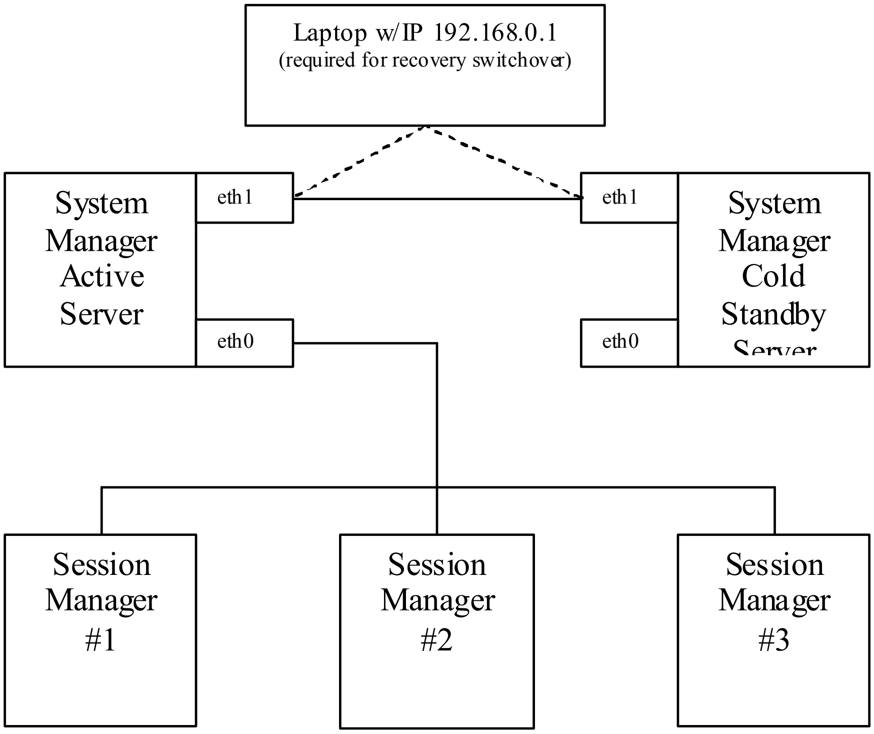
The upgrade procedures for Service Pack 1 are described in *Upgrading Avaya Aura*^{TM} *Session Manager Service Pack 1* at http://support.avaya.com

Chapter 18: Cold Standby - Replace System Manager

The cold standby recovery procedure allows an active System Manager server to be replaced with another physical server in the event that the active server becomes inoperable. This is essentially a second Linux server with the same hostname and network configuration (FQDN, IP Address, etc), that is not connected to the active network until it is needed due to a failure occurring on the primary System Manager server.

Cold Standby server requirements

Each System Manager server must adhere to at least the minimum server requirements defined in the installation documentation. Each server must have at least two Ethernet network interface ports. The first Ethernet port (eth0) will be used to communicate with managed elements on the network. The second Ethernet interface (eth1) should be configured to allow the servers to talk directly via a crossover cable connecting the two servers.


Laptop w/IP 192.168.0.1
(required for recovery switchover)
System Manager Active Server
eth1
eth0
eth1
eth0
System Manager Cold Standby Server
Session Manager #1
Session Manager #2
Session Manager #3

Note in the diagram above, only the **active** System Manager server (eth0) is connected to the management network. This avoids IP address conflicts between the active and standby servers. If both servers were to be connected to the network at the same time, unexpected behavior could occur on the System Manager and associated Session Manager servers.

The eth1 network connecting the active and standby System Manager servers should be an isolated private network (suggested use is a single network crossover cable between the two servers), with different IP addresses administered on the eth1 interfaces on each System Manager server allowing communication between the two servers. This is the network connection that will be used to copy the active server backup files to the cold standby server.

Installation procedure

The installation procedure is:

1. Ensure both System Manager servers and all associated Session Manager servers have the same version of software. ***Mismatches in software versions will cause failures in the backup/recovery of the cold standby process.***
2. Configure the same System Name (hostname), FQDN, and IP address configuration on both System Manager Servers (ensure the following files have identical network configuration between both System Manager servers:
   - /etc/sysconfig/network – ensure HOSTNAME entry is identical
   - /etc/hosts – ensure the entry with the common IP address between the two systems contains the FQDN and the hostname and is a separate line from the looparound/ localhost IP address.
   - /etc/sysconfig/network-scripts/ifcfg-eth0 – ensure BOOTPROTO, IPADDR, NETMASK, and GATEWAY parameters in this file are identical.
3. Configure a common Linux OS-level account on both servers to be used for doing remote copies of backup files to the other server. It is suggested to use the ‘smbackup’ login for this purpose, with a home directory of /home/smbackup. Ensure the password set for this login contains at least 8 characters. To easily create this login and set its password on the System Manager server, log into the system as root, and execute the following commands from a bash shell prompt:

   ```
   # useradd smbackup
   # passwd smbackup
   ```

4. Configure the eth1 interfaces on both servers to use different IP addresses such that the two systems can talk to each other over the eth1 interfaces. It is suggested for this purpose that servers be given the following configuration on the eth1 interfaces:

Parameter	System Manager Server #1	System Manager Server #2
IP Address	192.168.0.2	192.168.0.3
Netmask	255.255.255.0	255.255.255.0

5. Connect the two eth1 interface ports with a crossover Ethernet cable, and verify that the servers are talking by **ping**’ing the IP address of the remote System Manager server from the local console.
6. Log into the System Manager Common Console on System Manager server #1.
7. Click **Settings > Backup and Restore** in the left navigation pane, click on the **Backup** button, and configure the remote backup details as shown below:

Field Name	Value
Type	Select the **Remote** radio button
SCP Server IP	192.168.0.3
SCP Server Port	22
User Name	smbackup (or whatever login was created above in step #3)
Password	Enter the password associated with the login created in step #3.
Filename	sysmgr-backup

8. Click on the **Schedule** button to bring up the scheduling page. Populate the fields on the scheduling page with the following information, and click on **Commit.**

Field Name	Value
Job Name	Periodic Cold Standby Backup
Task Time	Select time of day when System Manager usage will be minimal (i.e., 3:00 AM)
Recurrence	Select **Tasks are repeated Daily Every 1 Day(s)**
Range	Select **No End Date**

9. Log into the Common Console Management web interface on System Manager server #2.

10. Click **Settings > Backup and Restore** in the left navigation pane, click on the **Backup** button, and configure the remote backup details as shown below:

Field Name	**Value**
Type	Select the **Remote** radio button
SCP Server IP	192.168.0.2
SCP Server Port	22
User Name	smbackup (or whatever login was created above in step #3).
Password	Enter the password associated with the login created in step #3.
Filename	sysmgr-backup

11. Click on the **Schedule** button to bring up the scheduling page. Populate the fields on the scheduling page in the following fashion, and click on **Commit.**

Field Name	**Value**
Job Name	Periodic Cold Standby Backup
Task Time	Select time of day when System Manager usage will be minimal (i.e. 3:00 AM)
Recurrence	Select **Tasks are repeated Daily Every 1 Day(s)**
Range	Select **No End Date**

The above configuration will periodically backup the System Manager system on each server and use scp to copy the backup file to the other server.

Activation of Cold Standby server due to active failure

In the event that a failure to the active System Manager server occurs, the following procedure should be used to activate the cold standby server.

1. Log into the standby System Manager server via the console, or via an SSH client on the laptop as the backup user (i.e. smbackup in the examples above).
2. Once logged in at a bash prompt, use the **`ls –ltr`** command to list all the backup files in the directory where the backups were transferred. In the example above, backups were placed in /home/smbackup, so the command would be:
   `ls –ltr /home/smbackup/sysmgr-backup*` The format of the filenames in the case

of our example above will be ***sysmgr-backup_############.zip*** where the #'s represent a scheduled job number within the System Manager framework. The last file displayed in the list from the above **`ls`** command will be the most recent backup file, and is the one that should be used in step 8 below.

3. If the System Manager server has a graphical desktop system and has Firefox installed, then you can access the Common Console Management web interface from the System Manager console with Firefox accessing the URL http://127.0.0.1/IMSM. If this is the case, then continue with step 6.
4. Unplug the crossover cable from the eth1 port of the failed System Manager server and plug it into the services laptop with an IP address of 192.168.0.1 and a netmask of 255.255.255.0.
5. Launch the IE or Firefox browser on the laptop with the URL http://192.168.0.2/IMSM for server #1, or http://192.168.0.3/IMSM for server #2, depending upon which one you are going to restore on.
6. Log into the System Manager Common Console of the standby server.
7. Click on **Settings > Backup and Restore** in the left navigation pane, and click on the **Restore** button.
8. Select Type of **Local** and for filename enter the full pathname of where the backup file was stored from the remote system (i.e. /home/smbackup/sysmgr-backup_1240264801712), and click on the **Restore** button. The server will be restored with the selected remote backup from the other server. The web console will remain inaccessible during the restore process.
9. Once the web console becomes available again, the restore is complete. The Ethernet cable plugged into the eth0 port of the failed System Manager server should be moved to the eth0 port of the standby server. At this point, this server is now the active System Manager server.
10. Lastly, unplug the Ethernet cable from the laptop and restore it to its original configuration connecting the two eth1 ports of the System Manager servers so that future backups done on the new active server will get pushed to the new cold standby server.

Backup file maintenance on System Manager server

If you choose to do the scheduled backup files on the System Manager server since the filename is dependent upon the scheduled job, you need to delete older backup files from the system. This can be done manually, or scheduled through the cron system scheduler on the Linux server.

The following command will clean up backup files older than 30 days:

```
# find /home/smbackup –name '*.zip' –mtime +30 –exec rm –f {} \;
```

Chapter 19: Postgres database problems

After a power failure or database crash, the Postgres database may become corrupted and the Postgres server may not restart.

The recovery action is to clear the Write-Ahead Log (WAL) and optionally reset other control information using the **pg_resetxlog** command. Write-Ahead Logging is a standard method for ensuring data integrity. Changes to data files must be written only after those changes have been logged, that is, after log records describing the changes have been copied to permanent storage. In the event of a crash, the database can be recovered using the log. Any changes that have not been applied to the data files can be recovered from the log records.

pg_resetxlog

pg_resetxlog resets the write-ahead log and other control information of a PostgreSQL database cluster.

Syntax

```
pg_resetxlog [-f] [-n] [-o oid] [-x xid] [-e xid_epoch] [-m mxid]
[-O mxoff] [-l timelineid,fileid,seq] datadir
```

-f - force **pg_resetxlog** to proceed anyway if it complains that it cannot determine valid data for **pg_control**

-n - print the values reconstructed from **pg_control** and then exit without modifying any values. This option is mainly used for debugging, but may be useful as a sanity check before allowing **pg_resetxlog** to proceed for real.

-o oid - manually set the next OID

-x xid - manually set the next transaction ID

-e xid_epoch - manually set the next transaction ID's epoch

-m mxid - manually set the next multitransaction ID

-O mxoff manually set the next multitransaction offset

-l timelineid,fileid,seg manually set the Write-Ahead Log starting address

datadir - data directory (required)

Description

pg_resetxlog resets the write-ahead log and other control information stored in the **pg_control** file. It should be used only as a last resort when the server will not start due to database corruption.

pg_resetxlog can only be run by the user who installed the server because it requires read/write access to the data directory. For safety reasons, you must specify the data directory on the command line.

The recovery actions are:

1. Try restarting the PostgreSQL service
2. Backup the Postgres database
3. Run **pg_resetxlog**

After running **pg_resetxlog**, it should be possible to start the server, but the database may contain inconsistent data due to partially-committed transactions. If this is the case, you should:

- immediately dump the data. ***Do not*** execute any data-modifying operations in the database before you do the dump, since any action is likely to make the corruption worse.
- run **initdb** and note the environment variables such as LANG, etc.
- reload

After reloading, check for inconsistencies and repair as needed.

Problems running pg_resetxlog

pg_resetxlog won't start

This command will not run when the server is running. **pg_resetxlog** will refuse to start if it finds a server lock file in the data directory. If the server crashed, a lock file may have been left behind. In that case, you should:

- make certain that there is no server process still alive
- remove the lock file to allow **pg_resetxlog** to run

pg_resetxlog cannot determine valid data

If **pg_resetxlog** complains that it cannot determine valid data for **pg_control**, you can force it to proceed anyway with the **-f** option. Plausible values will be substituted for the missing data. Most of the fields will match, but manual assistance may be needed for the next OID, next transaction ID and epoch, next multitransaction ID and offset, WAL starting address, and database locale fields using the options above. If you are not able to determine the correct values for all of these fields, `-f` can still be used, but the recovered database may still be corrupted. Safe values for the fields can be determined as follows (file names are in hexadecimal):

- A safe value for the next transaction ID (-x) may be determined by:
  - looking for the numerically largest file name in the directory **pg_clog** under the data directory
  - adding 1
  - multiplying by 1048576 (five trailing zeroes provide the proper multiplier)
  - Example: if 0011 is the largest entry in **pg_clog**, enter `pg_resetxlog -x 0x120000`
- A safe value for the next multitransaction ID (-m) may be determined by:
  - looking for the numerically largest file name in the directory **pg_multixact/offsets** under the data directory
  - adding 1
  - multiplying by 65536 (four trailing zeroes provide the proper multiplier)
  - Example: if 0011 is the largest entry in **pg_multixact/offsets**, enter `pg_resetxlog -x 0x120000`
- A safe value for the next multitransaction offset (-O) may be determined by:
  - looking for the numerically largest file name in the directory **pg_multixact/members** under the data directory
  - adding 1
  - multiplying by 65536 (four trailing zeroes provide the proper multiplier)
  - Example: if 0011 is the largest entry in **pg_multixact/members**, enter `pg_resetxlog -x 0x12000`
- The WAL starting address (-l) should be larger than any file name currently existing in the directory **pg_xlog** under the data directory. The names have three parts:
  - The first part is the "timeline ID" and should not be changed.
  - The second part should not be changed
  - The third part should be incremented by 1. The value cannot be larger than 255 (0xFF). If adding 1 to the third part causes the value to be larger than 0xFF, increment the second part by 1 and reset the third part to 0. For example, if 00000001000000320000004A is the largest entry in **pg_xlog**, enter `pg_resetxlog -l 0x1, 0x32, 0x4B.` If 000000010000003A000000FF is the largest entry, enter `pg_resetxlog -l 0x1, 0x3B, 0x0.`
- There is no easy way to determine a next OID, but it is not critical to set the next OID correctly.
- The transaction ID epoch is not stored anywhere in the database except in the field that is set by **pg_resetxlog**, so any value will work.

References

For more information regarding data integrity on Postgres, see http://www.postgresql.org/docs/8.1/static/wal.html#WAL_RELIABILITY

For more information regarding **`pg_resetxlog`** see http://www.postgresql.org/docs/8.2/static/app-pgresetxlog.html

Appendix A: Log and Alarm Event IDs

Event ID Format

Event IDs use the format *<SP><X[YYY][#####]>*. Some examples of possible Event IDs are:

OP_APRX10011

AU_MEMG20100

SP is the Standardized Prefix, and can be one of the following:

Prefix	**Description**
AU_	audit trail
OP_	operational, including error and performance
SE_	security records
TR_	trace and debug

X is a single capital letter which indicates a major Session Manager functional category:

G	General
A	ASSET (SM100)
M	Management
C	Call Processing

YYY are three capital letters which indicate a sub-category, if needed. Some examples are:

AAPX	SM100 ASSET Proxy
AFWL	SM100 ASSET Firewall
AHWM	SM100 ASSET Test
CMON	CP SIP Monitor
CSRE	CP SRE
MSEM	Management Session Manager Element Manager
MAMA	Management SM100 Management Agent

##### are 5 digits for event IDs within an area. Each area has a unique number range, such as:

SM100	10000-19999
Call Processing	50000-59999

Alarm Procedures

Alarms are not automatically acknowledged or cleared. When a new alarm appears on the **Alarm Viewer** screen, you need to:

1. Change the status of the alarm to **Acknowledged**. On the System Manager console, click on **Monitoring > Alarming**. Select the appropriate alarm(s), click on the **Change Status** button, and select **Acknowledged** from the drop-down menu.
2. Check the log event list to see if the alarm has an associated clear event code. Some alarms have no clear event code such as OS or platform alarms. On the System Manager console, click on **Monitoring > Logging.** Using the **Display filter** option, enter the Event ID or part of the Event ID (OP_MMTC) in the filter field for Event ID.
    - If the alarm has an associated clear event ID, change the status of the alarm(s) to **Cleared**.
    - If the alarm does not have an associated clear event ID, look for the alarm code in the Log and Alarm Event ID Table and investigate how to troubleshoot the problem using the link in the Log Message/Alarm Description column.

Log Event and Alarm Event ID descriptions

The following table contains an alphabetical list of log and alarm event IDs, the level/severity of the log or alarm event, and either a description of the log event message or a link to the description of the alarm event and how to troubleshoot the alarm.

Log and Alarm Event ID Table

Event ID	Log/Alarm Severity	Log Message/ Alarm Description
AU_MSEM20304	INFO No alarm	LoginID: {1} ClientHost: {2} Action: Database UPDATE on table {3} with key {4} and properties: {5}
AU_MSEM20306	INFO No alarm	LoginID: {1} ClientHost: {2} Action: Database INSERT on table {3} with key {4} and properties: {5}
AU_MSEM20308	INFO No alarm	LoginID: {1} ClientHost: {2} Action: Database DELETE on table {3} with key {4} and properties: {5}
AU_MSEM20310	INFO No alarm	LoginID: {1 ClientHost: {2} Action on Session Manager: {6} Description: {7}
AU_MSEM20312	INFO No alarm	LoginID: {1} ClientHost: {2} Action on System Manager: {7}
OP_AAPX10800	INFO No alarm	Connection established to SD or IH, IP=#ip address port=#port transport =(TCP|TLS|UDP) Connection Status
OP_AAPX10801	INFO No alarm	Connection broken to SD or IH, IP=#ip address port=#port transport =(TCP|TLS|UDP) Connection Status
OP_AAPX10802	INFO No alarm	Connection broken to TH, IP=#ip address port=#port transport =(TCP|TLS|UDP) Connection Status
OP_AASL10900	ERROR Minor	Certificate load failure certificate type=(Identity|CA) Certificate Status
OP_AASL10901	INFO No alarm	Certificate load success certificate type=(Identity|CA) Certificate Status
OP_ACLB10002	INFO No alarm	Board cold boot Board Running Status
OP_ACLB10003	INFO No alarm	Board restart Board Running Status

Log and Alarm Event ID Table		
Event ID	**Log/Alarm Severity**	**Log Message/ Alarm Description**
OP_ACLB10004	INFO No alarm	Board stop Board Running Status
OP_AFWL15001	INFO No alarm	SIP Firewall new configuration imposed SIP Firewall Configuration
OP_AFWL15002	INFO No alarm	Busyout mode is ON | OFF SIP Firewall Configuration
OP_AFWL16001	INFO No alarm	SIP firewall deep inspection disabled or no active rules SIP Firewall Configuration
OP_AFWL16002	ALERT	SIP firewall deep inspection configuration update failed (rule #, <rule name string>), retaining existing configuration SIP Firewall Configuration
OP_AFWL16003	ALERT	SIP firewall configuration failed schema validation SIP Firewall Configuration
OP_AFWL16501	ALERT	SIP firewall action <ALERT|PERMIT|DROP|RATE-LIMIT|RATE-BLOCK> message (length:#) - matched rule: <rulename>, [optional message,] <TCP|TLS|UDP>, remote <addr:port#>, local <addr:port#> SIP Firewall Actions
OP_AFWL16502	INFO No alarm	SIP firewall action <ALERT|PERMIT|DROP|RATE-LIMIT|RATE-BLOCK> message (length:#) - matched rule: <rulename>, [optional message,] <TCP|TLS|UDP>, remote <addr:port#>, local <addr:port#> SIP Firewall Actions
OP_AFWL17501	INFO No alarm	SIP firewall blacklist disabled or no active rules SIP Firewall Configuration
OP_AFWL17502	INFO No alarm	SIP firewall whitelist disabled or no active rules SIP Firewall Configuration
OP_AFWL17503	ALERT	SIP firewall blacklist configuration update failed (network rule # | content rule #), retaining existing configuration SIP Firewall Configuration
OP_AFWL17504	ALERT	SIP firewall whitelist configuration update failed (network rule # | content rule #), retaining existing configuration SIP Firewall Configuration

Log and Alarm Event ID Table

Event ID	Log/Alarm Severity	Log Message/ Alarm Description
OP_AHWM10100	ALERT	Board overheating event (yellow zone) Board Temperatures
OP_AHWM10101	CRITICAL Major	Board overheating event (red zone) Board Temperatures
OP_AHWM10102	INFO No alarm	Temperature normal Board Temperatures
OP_AHWM10103	INFO No alarm	90 percent of total memory was consumed Board Memory
OP_ANFW11000	INFO No alarm	Network firewall started
OP_ANFW11001	WARN Warning	Network firewall stopped
OP_APLM10300	ERROR Minor	Failure pinholing Network Firewall, interface=(intf|all) port=#port transport=(TCP|TLS|UDP) Network Firewall Pinholing
OP_APLM10301	INFO No alarm	Success pinholing Network Firewall, interface=(intf|all) port=#port transport=(TCP|TLS|UDP Network Firewall Pinholing
OP_APLM10302	ERROR Minor	Failure configuring network parameters Network Configuration
OP_APLM10303	INFO No alarm	Success configuring network parameters Network Configuration
OP_APLM10304	ERROR Minor	Eth(0) interface is down Network Configuration
OP_APLM10305	INFO No alarm	Eth(0) interface is up Network Configuration
OP_ASMT10700	INFO No alarm	Start sip trace SIP Tracing
OP_ASMT10701	INFO No alarm	Stop sip trace SIP Tracing
OP_AWTC10400	ERROR Minor	Application <name> restart failure Application Failure
OP_AWTC10405	WARNING	Identity certificate is about to expire Certificate Expiration

Log and Alarm Event ID Table		
Event ID	**Log/Alarm Severity**	**Log Message/ Alarm Description**
OP_AWTC10406	ALERT	Identify certificate expired Certificate Expiration
OP_CDAO50001	ERROR Minor	The database connection is down. Administration updates will not function during this outage. Database Connection
OP_CDAO50002	ERROR Minor	Administration relating to the <admin> screen(s) may have caused a database query failure (SQL Exception). The failing object was the <object>. Database Query
OP_CDAO50003	ERROR Minor	Administration relating to the <admin> screen(s) may have caused the database to become corrupt. The failing object was the <object> Database Corrupted
OP_CDAO50004	WARN Warning	The database connection is currently down. Trying again <warning count> more times before alarming an error. Database Connection
OP_CDAO50005	INFO No alarm	The database connection has been restored. Administration updates should be taking effect now. Database Connection
OP_CDAO50006	INFO No alarm	There is corrupt data in the database relating to the <admin> screen(s), for the <class> class. Database Connection
OP_CDAO50007	INFO No alarm	There was corrupt data in the database for relating to the <admin> screen(s), but it has been corrected in the <class> class. Database Corrupted
OP_CDAO50008	INFO No alarm	There was an SQL query error relating to the <GUI> screen(s) for the <class> class, but it has been corrected. Database Query
OP_CDAO50009	ERROR Minor	A file I/O error for <file> occurred trying to write the local DNS server configuration or zone files. Zone File I/O
OP_CDAO50010	INFO No alarm	There was a file I/O error for <file>, but it has been corrected. Zone File I/O

Log and Alarm Event ID Table		
Event ID	**Log/Alarm Severity**	**Log Message/ Alarm Description**
OP_CDAO50011	ERROR Minor	The Session Manager Instance cannot be resolved. Double check the administration on the <admin> screen(s). Session Manager Instance Resolution
OP_CDAO50012	ERROR Minor	Multiple Session Manager IP addresses map to the local Session Manager Instance. Double check administration screen(s) <admin>, or real DNS such as /etc/hosts. For now, choosing entity <sip entity name>. Session Manager Instance Resolution
OP_CDAO50013	ERROR Minor	DNS resolved to multiple IP addresses for SM100; choosing address <ip address>. SM100 Multiple DNS Resolutions
OP_CDAO50014	WARN Warning	A file I/O error for <file> occurred trying to write the local DNS server configuration or zone files. Attempting <warning count> more times to correct. Check the file permissions, directory existence, disk space, etc. Zone File I/O
OP_CDAO50016	INFO No alarm	The Session Manager Instance resolution issue has been corrected. Session Manager Instance Resolution
OP_CDAO50017	INFO No alarm	DNS no longer resolves to multiple IP addresses for the SM100. SM100 Multiple DNS Resolutions
OP_CDAO50018	WARN Warning	Bandwidth threshold exceeded for the <location name> location. Used/allowed bandwidth: <used>/<allowed> Exceeding Location Bandwidth
OP_CDAO50019	INFO No alarm	Bandwidth threshold no longer exceeded for the <location name> location. Exceeding Location Bandwidth
OP_CDAO50020	ERROR Minor	There is a problem with the Call Detail Recording (CDR) system. Call accounting is not operational. CDR Not Operational
OP_CDAO50021	INFO No alarm	The Call detail Recording (CDR) system is now operational. Call accounting is resumed. CDR Not Operational

Log and Alarm Event ID Table		
Event ID	**Log/Alarm Severity**	**Log Message/ Alarm Description**
OP_CDAO50022	WARN Warning	The direct link for Session Manager to Route-Through using the Entity Link to <session manager name> on port <port number> using <port number> is missing. Double check the administration on <admin> screen(s) to correct. Route Through
OP_CDAO50023	INFO No alarm	The missing Entity Link for Session Manager to Route-Through to <session manager name> has been inserted. Route Through
OP_CMON55000	INFO No alarm	SIP monitoring state for entity < entity name> is no longer <entity state>. SIP Monitor Alarm
OP_CMON55001	WARN Warning	SIP monitoring state for entity < entity name> is <entity state>. SIP Monitor Alarm
OP_CMON55002	WARN Warning	SIP monitoring state for entity <entity name> is <entity state>. SIP Monitor Alarm
OP_CSRE52000	INFO No alarm	<extension module> extension module now working properly and is deployed. Extension Module Deployment
OP_CSRE52003	ERROR Minor	Attempted DNS resolution while extension module was not deployed. Extension Module Deployment
OP_MAMA20100	ERROR Minor	Security Module Management Agent is unable to connect to SIP A/S Management Server
OP_MAMA20101	INFO No alarm	Security Module Management Agent connected to SIP A/S Management Server
OP_MAMA20102	ERROR Minor	Security Module Management Agent is not able to configure SM100
OP_MAMA20103	INFO No alarm	Security Module Management Agent is able to configure SM100.
OP_MMTC20011	ERROR Minor	Postgres database sanity check failed; the database is unaccessible
OP_MMTC20012	INFO No alarm	Postgres database sanity check passed

Log and Alarm Event ID Table		
Event ID	**Log/Alarm Severity**	**Log Message/ Alarm Description**
OP_MMTC20013	ERROR Minor	Service Host sanity check failed; call processing is down
OP_MMTC20014	INFO No alarm	Service Host(s) sanity check passed
OP_MMTC20015	ERROR Minor	Session Manager sanity check failed; call processing is down.
OP_MMTC20016	INFO No alarm	Session Manager sanity check passed.
OP_MMTC20017	ERROR Minor	Management Server sanity check failed; SIP A/S admin is unavailable
OP_MMTC20018	INFO No alarm	Management Server sanity check passed
OP_MMTC20019	ERROR Minor	SAL-Agent sanity check failed; alarms are not being processed
OP_MMTC20020	INFO No alarm	SAL-Agent sanity check passed
OP_MMTC20021	ERROR Minor	Management jboss sanity check failed; services are unavailable
OP_MMTC20022	INFO No alarm	Management jboss sanity check passed
OP_MMTC20023	ERROR Minor	System Replication sanity check failed
OP_MMTC20024	INFO No alarm	System Replication sanity check passed
OP_MMTC20025	ERROR Minor	SM100 sanity check failed; call processing is down
OP_MMTC20026	INFO No alarm	SM100 sanity check passed
OP_MMTC20027	ERROR Minor	System Manager Replication test failed
OP_MMTC20028	INFO No alarm	System Manager Replication test passed
OP_MMTC20029	ERROR Minor	Call Processing SAR is not deployed

Log and Alarm Event ID Table		
Event ID	**Log/Alarm Severity**	**Log Message/ Alarm Description**
OP_MMTC20030	INFO No alarm	Call Processing SAR is deployed successfully
OP_MMTC20031	ERROR Minor	Data Distribution/Redundancy is down.
OP_MMTC20032	INFO No alarm	Data Distribution/Redundancy is up.
OP_MWD20200	INFO No alarm	Service <service name> has started.
OP_MWD20201	ERROR Minor	Service <service name> has died.
OP_MWD20202	ERROR Minor	Service <service name> failing to start after several attempts

Notes:

1. Login name
2. IP address of client’s web browser connection to System Manager
3. Database table name
4. Key name
5. List of properties
6. Session Manager instance name
7. Action description

Board Running Status

These events are normal and report the last known running state of the SM100 card. When the SM100 successfully boots, is restarted, or has been stopped, the respective log message is sent to System Manager. No action is required.

Board Temperatures

When the SM100 card reaches a temperature above its expected normal operating range, a *yellow zone* warning alarm is sent to System Manager. If the temperature continues to rise to a critical level such that the SM100 might be damaged, a *red zone* danger alarm is sent to System Manager. These alarms will continue to be sent until the temperature of the SM100 returns to normal, at which time a *temperature normal* log message will be sent to indicate the problem has been resolved. The alarm status can be changed to **Cleared**.

Required action: if *yellow zone* or *red zone* alarms are observed, either the Session Manager hardware hosting the SM100 is not getting proper ventilation, or the SM100 card is failing.

- Verify that there are no blockages of air inlets to the Session Manager hardware.
- Verify that external climate-control systems are functioning properly.

If the temperature does not return to normal, it may be that the Session Manager cooling fans have failed or the SM100 card is in danger of failing. Contact Avaya Technical Support for repair or replacement.

Board Memory

Under normal situations, the SM100 is capable of running with installed memory. However, memory leakage may cause unnecessary consumption of memory. If this occurs, a log message is sent to the System Manager.

If the problem persists, contact Avaya Technical Support.

Network Firewall Pinholing

By default, the SM100 network firewall restricts access to all but those interfaces/ports defined in the *Avaya Aura Session Manager: Port Matrix:* documentation (available by logging into the support website and using the InSite Knowledge Management Database at http://support.avaya.com). However, the pinhole mechanism permits applications to make on-demand requests to open (close) temporary “pinholes” through the network firewall. The result of these requests is logged to System Manager. Information contained in the message identifies the network interface (specific interface or all interfaces), the port that is being opened, and the transport protocol to which the port is associated.

Failure of an application to open a pinhole indicates an internal Session Manager problem. If this problem persists, contact Avaya Technical Support.

Network Configuration

During installation and administration of Session Manager, the SM100 network parameters are configured. Both successful and unsuccessful configurations are reported. If the SM100 network cannot be configured, an alarm is sent to System Manager.

When the SM100 is stopped or restarted, you will see the SM100 public interface (Eth0) change state between up and down. During normal operation, the interface should be up only.

Failure to properly configure the SM100 network may be the result of incorrect settings. Check the configuration and try resetting the SM100. If this does not resolve the problem, there may be an internal Session Manager problem. If the problem persists, contact Avaya Technical Support.

Application Failure

If an SM100 application fails to start or restart, this may indicate a problem with SM100 resources (i.e. memory), a configuration issue, or a problem with the application itself. The name of the application which fails to start is shown in the log message

If this problem persists, review the log to determine if any other problems might be affecting the application's ability to load (e.g., 90% memory consumed). Otherwise, this is an internal software problem. Contact Avaya Technical Support.

Certificate Expiration

The SM100 requires a certificate for securing SIP connections. If this certificate has expired, the SM100 will not be able to establish any new SIP TLS connects, and security will be compromised. In many cases, TCP and UDP are not options, so it is imperative that certificate lifetime be monitored.

When the SM100 certificate is approaching its expiration, a warning message is periodically logged starting 30 days before expiration. If the certificate has expired, a daily alarm is sent to System Manager. Refer to *Installing and Administering Avaya Aura*$^{\text{TM}}$ *Session Manager, 03-603324* for instructions for getting a new certificate.

SIP Tracing

Session Manager provides a tool for tracing SIP messages (see Tracing). When tracing is started or stopped, a log message is sent to System Manager. No action is required. Note that SIP tracing may impact SM100 performance in some cases and normally should be turned off.

Connection Status

The state changes of Session Manager connections are logged to System Manager. The specific hosts reported are:

- Trusted SIP Entities (also referred to as Trusted Hosts)

- Service Director (SD)
- Service Hosts (SH, also called Instance Hosts, IH).

Trusted SIP Entity examples are Avaya Communication Manager and CLAN. SD and SH are components of the Session Manager SIP Server. Information contained in these log messages includes host IP address, port, and the transport protocol associated with the port. This information can be used to diagnose network wiring or network configuration problems (host interface, protocol, address/mask assignment, etc.)

In the case of Trusted SIP Entities, a connection failure log message may indicate that certificate maintenance is required or that the Credential name in the Network Routing Protocol is configured incorrectly.

Certificate Status

The SM100 identity certificate and CA (trusted) certificate must be present for SIP TLS. If one of these certificates cannot be loaded (i.e., the certificate is invalid, expired, revoked), an alarm is sent to System Manager.

Make sure that valid identity and CA certificates are installed on the system. See also Certificate Expiration in this document and Trust Management in *Installing and Administering Avaya Aura*^{TM} *Session Manager, 03-603324.*

SIP Firewall Configuration

Changes to the SM100 SIP firewall configuration are always reported to System Manager. Most of the messages are informational (configuration successful, ruleslist/blacklist/whitelist disabled). However, configuration failures are serious and cause alarms. When alarms are generated, information about the failure is provided: effected list, list rule number, and some rule details.

Configuration failure is not an expected occurrence. Refer to the SIP Firewall Configuration section of *Installing and Administering Avaya Aura*^{TM} *Session Manager, 03-603324* to ensure that the rule is correctly configured. If the problem persists, report the problem to Avaya Technical Support.

SIP Firewall Actions

If administration has configured SIP firewall rules with logs or alarms, all received SIP messages matching that rule will cause System Manger to be notified. These log/alarm messages are rate-limited to prevent Denial of Service attacks on the logging/alarming systems.

Information contained in the log/alarm message includes the action taken on the SIP message, matched rule name, an administration-customized message, the transport protocol over which the message was received, originating host address/port, and destination host address/port.

These logging details can be used to further analyze and mitigate threats to the system. If too many “matched-rule” log/alarm messages are received, review them and consider additional changes to the SIP Firewall configuration to reduce messages. Refer to the SIP Firewall Configuration section of *Installing and Administering Avaya Aura*TM *Session Manager, 03-603324.*

Database Connection

This is related to the database which contains the administered data for routing, users, etc. This alarm means that the connection to the database is either timing out or has been lost. During this outage, any new administration will not be recognized by the running system.

Causes:

- The connection to the database has been lost or is experiencing timeouts between queries.
- The database may not be running on the Session Manager or is on a different IP address than expected.
- The database process may not be running.

Corrective actions:

- Ensure there is an actual connection to the database. Also check that this connection is stable and not experiencing outages. Ensure the Session Manager is reachable by pinging it from another machine that should be able to reach it:
    - *ping w.x.y.z* where w.x.y.z is the IP address of the Session Manager.
    - If there is no answer, the system is either in an unresponsive state, is currently off, or is in the middle of a reboot.
- Ensure the Session Manager IP address or DNS name is configured properly for the running Instance. This requires root access.
- Ensure the database process is running on the Session Manager. This action requires root access.
- Make sure the database user name and passwords match the default values provided by the system. Contact Avaya Technical Support.

Database Query

This event occurs when a database query cannot complete or experiences a failure. This would likely only be seen after an upgrade which would indicate that the upgrade had problems. As a result, the Session Manager will likely not behave correctly or at all.

This event can occur if the database schemas do not match, indicating that variable types are different, fields are non-existent, etc. For example, an Integer type column becomes a Boolean type.

Call Avaya Technical Support to check the database versions and to ensure they are correct and compatible. In particular, the table *schemaversion* in the System Manager and Session Manager databases should have appropriate and matching version entries in the major, minor, revision, and schemaname columns.

Database Corrupted

Corrupted or bad data has been copied into the database. Components of Session Manager which depend on this data will likely not be operating properly.

This event may be caused by administration which contained bad data that was not properly checked for errors. This event can also occur if someone writes directly into the database. An example would be if someone enters a digit pattern “5555” but sets the minimum and maximum limits to 3. They should both be at least 4.

To correct this problem, check any recent administration relating to the alarm’s suggested configuration pages. If nothing appears out of the ordinary, contact Avaya Technical Support.

Zone File I/O

Zone files are written to the local file system to reflect the host name resolution data administered on the Local Host Name Resolution page. The SM100 uses that data when performing DNS resolution.

A Zone File I/O alarm indicates that an error occurred while trying to access the file system to read or write data for zone files.

Causes may include:

- Missing directories
- Permission errors
- No space on the disk
- Other errors which cause a read or write to the zone files to fail.

To fix the problem:

- Ensure there is space on the disk. Execute **`df`** and make sure that the **Use%** value is not greater than 95%.
  - If the **Use%** value is greater than 95%, remove any unnecessary large files and old log files on the system.
- Ensure that the file */etc/named.nre.zones* exists and has read permissions for all users plus write permissions only for the owner, root (-rw-r--r--).
  - If the file does not exist or the permissions are incorrect, contact Avaya Technical Support.

Session Manager Instance Resolution

This event occurs when the IP address of the configured Session Manager does not match the administration of any Session Manager instance. During this failure, the Session Manager will not service any calls.

Possible causes:

- No Session Manager that is administered in System Manager has a Management Access Point Host Name/IP address that matches the Session Manager instance's IP address. This could be an administration error, possibly due to entering the IP address of the SM100 by mistake.
- A DNS name is resolving to multiple IP addresses or to no IP address.

To fix the problem:

- Enter a correct IP address in the Session Manager Administration's Management Access Point Host Name/IP field.
- If the Management Access Point Host Name/IP is a DNS name, check to what it resolves using the command **`host someDNSname`** where **`someDNSname`** is the server name. Check */etc/hosts* on the Session Manager to ensure that the name resolves to one IP address. The file should have entries in the form of **<IP Address> <fully qualified domain name> <domain>.** Change the DNS to resolve to exactly one IP address if necessary.

SM100 Multiple DNS Resolutions

The SM100 is provisioned as a DNS name in the Session Manager, but the name resolves to more than one IP address. The default behavior is to use the first IP address that the DNS name maps to, which may cause unintended behavior. The system may appear to operate normally; however, behavior may be very unreliable.

To correct this problem:

- Change the DNS resolution by either entering an IP address in the Session Manager's SM100 administration, or make the DNS name resolve to a single IP address.
- Check what the name resolves to using the command `host someDNSname` where `someDNSname` is the server name.
- Check */etc/hosts* to ensure that the name, if it appears here, resolves to one IP address. The file should have entries in the form of
  <IP Address> <fully qualified domain name> <domain>

Exceeding Location Bandwidth

This event is related to the Call Admission Control functionality for the SIP Routing Element (SRE), a component of Session Manager. This event indicates that the used bandwidth for a specific Location has consistently exceeded a pre-defined high threshold (currently, 90% of the bandwidth capacity), or that no more usable bandwidth is available for calls using that specific Location (bandwidth is at 100% capacity).

When the bandwidth is at 100% capacity for a particular Location, new calls are not allowed to or from that Location and will be denied.

This event may be caused by one of the following:

- There is more simultaneous call traffic than anticipated at a specific Location.
- The provisioned bandwidth for a specific Location is insufficient for the actual carried traffic.
- The provisioned bandwidth for a specific Location is correctly set according to LAN characteristics, but traffic exceeds actual network capacity.

To fix the problem:

- Ensure the traffic is consistent with the bandwidth capacity.
- Consider rerouting part of the traffic through a different, under-utilized Location.
- Increase bandwidth provisioning if allowed by the network.
- Consider splitting the Location into two or more different Locations and route traffic accordingly.

CDR Not Operational

This event is related to the Call Detail Recording (CDR) functionality for the SIP Routing Element (SRE), a component of Session Manager. This event means that call accounting is not available for calls to or from certain SIP entities for which CDR is enabled. During this outage, some or all calls will not be recorded in CDR.

Possible causes include:

- The CDR Extension Module is unable to process CDR call events
- The CDR Extension Module may not be running.

If the problem persists, contact Avaya Technical Support.

Route Through

This event indicates that Route Through is being attempted on calls, but it cannot route through to another Session Manager Instance. Calls may be denied as a result of not being able to Route Through. This may or may not be a real problem, depending on the customer's desired configuration.

The most likely cause is that the Entity Link between the Session Managers is missing in the NRP Entity Link page.

To fix this problem, add the correct Entity Link between the two Session Managers. The Alarm message should identify which Session Managers experienced the “Can't Route Through” problem.

Extension Module Deployment

This event indicates that the Extension Module described in the alarm log was not properly deployed. Currently, the only supported module which can produce this error is the DNS Extension Module. During this outage, any non-provisioned, DNS Fully Qualified Domain Names (FQDN) will not be resolved.

The DNS Extension Module is missing or is corrupted. Contact Avaya Technical support

SIP Monitor Alarm

SIP Monitoring has detected that the alarmed SIP entity is not successfully responding to SIP OPTIONS requests. A SIP entity may be reachable via several addresses, depending on Local Host Name Resolution administration and DNS address resolution. If the entity’s state is “down”, none of the entity’s addresses are responding to OPTIONS requests successfully. If the entity’s state is “partially up”, at least one of the entity’s addresses is responding successfully and at least one is not responding successfully.

The **SIP Monitoring Status** page on the System Manager will provide more detail, including the status of the entity’s various addresses and the response codes returned by the various addresses. The response codes are the standard SIP responses according to RFC 3261, section 21.

This event may be caused by the OPTIONS request not reaching the alarmed SIP entity because of problems with the network, or the alarmed SP entity may not be responding to the OPTIONS request.

To investigate this problem:

- Verify that network connectivity exists between the Session Manager and the alarmed SIP entity using the **`ping`** command.
- Using the SIP Tracer tool or a network protocol analyzer such as Wireshark, verify that an OPTIONS request is sent from the Session Manager to the alarmed entity, and that the entity responds successfully (typically with a “200 OK” response).

SM100 Sanity Failure

Use the Security Module Status screen to check the current status. Reset the Security Module if the error condition persists. The Security Module Status screen provides the reset capability.

Appendix B: Hard drive and environment events

The following table contains hard disk and environment monitoring alarms. All of the failure events are major alarms. The table contains information regarding the Event ID, a description of the Event ID, the cause, and recovery action(s).

The alarm message contains the disk number of the failing or failed drive. For example, an alarm message for Event ID 2048 would be:

```
Storage Service EventID: 2048 Device failed: Physical disk 0:0:1
Controller 0, Connector 0
```

Also, the LED display on the Avaya S8510 server indicates which disk failed or is failing.

Event ID	Description	Severity	Cause and Action
1354	Power supply detected a failure	Error	A power supply has been disconnected or has failed. The following information is displayed: • Sensor location (location in chassis) • Chassis location: (name of chassis) • Previous state was: (state) • Power Supply type: (type of power supply) • <Additional power supply status info) • Configuration error type: (if in configuration error state, type of configuration error)
2048	Device failed	Failure	A storage component such as a physical disk failed. Replace the failed component. Perform a rescan after replacing the disk.
2056	Virtual disk failed	Failure	One or more physical disks included in the virtual disk have failed. Replace the failed disk(s). Create a new virtual disk and restore from a backup.

Event ID	Description	Severity	Cause and Action
2057	Virtual disk degraded	Warning	There are two possible causes: Cause 1 - A physical disk included in a redundant virtual disk failed. Configure hot spare for the virtual disk if one is not already configured. Rebuild the virtual disk. when using an Expandable RAID Controller (PERC) PERC 3/SC, 3/DCL, 3/DC, 3/QC, 4/SC, 4DC, 4eDC, 4/Di, CERC ATA100/4ch, PERC5/E, PERC5/i or a Serial Attache SCSI (SAS) 5/iR controller, rebuild the virtual disk by first configuring a hot spare for the disk, then initiating a write operation to the disk. The write operation will initiate a rebuild of the disk. Cause 2: A physical disk in the disk group has been removed. If a physical disk was removed from the disk group, either replace the disk or restore the original disk. Perform a rescan after replacing the disk.
2076	Virtual disk check consistency failed	Failure	A physical disk in the virtual disk failed or there is an error in the parity information. Replace the failed physical disk. Rebuild the physical disk. When finished, restart the check consistency operation.
2080	Physical disk initialize failed	Failure	The physical disk has failed or is corrupt. Replace the failed or corrupt disk Restart the initialization.
2083	Physical disk rebuild failed	Failure	A physical disk in the virtual disk has failed or is corrupt. A user may also have cancelled the rebuild. Replace the failed or corrupt disk. Rebuild the virtual disk.
2102	Temperature exceeded the maximum failure threshold	Failure	The physical disk enclosure is too hot. There are several possible causes: a fan may have failed, the thermostat may be set too high, or the room temperature may be too hot. Check for factors which may cause overheating: l Verify that the fan is working l Check the thermostat settings l Check if the enclosure is near a heat source l Make sure the enclosure has enough ventilation l Make sure the room is not too hot l See the physical disk enclosure documentation for more diagnostic information
2103	Temperature dropped below the minimum failure threshold	Failure	The physical disk enclosure is too cool. Check if the thermostat setting is too low and if the room temperature is too cool.

Event ID	Description	Severity	Cause and Action
2107	Smart configuration change	Failure	A disk has received a SMART alert (predictive failure) after a configuration change. The disk is likely to fail in the near future. Replace the disk that has received the SMART alert. If the physical disk is a member of a non-redundant virtual disk, back up the data before replacing the disk.
2163	Rebuild completed with errors	Failure	In some situations, a rebuild may complete successfully while also reporting errors. This may occur when a portion of the disk containing redundant (parity) information is damaged. The rebuild process can restore data from the healthy portions of the disk but not from the damaged portion. 1. Back up the degraded virtual disk. - If the backup is successful, the user data on the virtual disk has not been damaged. Continue with Step 2. - If the backup encounters errors, the user data has been damaged and cannot be recovered from the virtual disk. In this case, the only possibility for recovery is to restore from a previous backup of the virtual disk. 2. Perform a consistency check on the virtual disk that you have backed up. 3. Restore the virtual disk onto the healthy array disks.
2169	The controller battery needs to be replaced.	Failure	The controller battery cannot recharge. The battery may be old or the charger may not be working. Replace the battery pack.
2268	%1 Storage Management has lost communication with the controller	Failure	Storage Management has lost communication with a controller. The controller driver or firmware may be experiencing a problem. The %1 is a substitution variable which displays text and varies depending on the situation. Reboot the system. If the problem is not resolved, contact Avaya Support.
2270	The physical disk Clear operation failed	Failure	A Clear task was being performed on a physical disk but the task did not complete successfully. The controller may have lost communication with the disk, the disk may have been removed, or the cables may be loose or defective. Verify that the disk is present and not in a Failed state. Make sure the cables are attached securely. Restart the Clear task.

Event ID	Description	Severity	Cause and Action
2272	Patrol Read found an uncorrectable media error	Failure	The Patrol Read task has encountered an error that cannot be corrected. There may be a bad disk block that cannot be remapped. Backup the data. If you are able to back up the data successfully, then fully initialize the disk and restore from back up.
2273	A block on the physical disk has been punctured by the controller	Failure	The controller encountered an unrecoverable medium error when attempting to read a block on the physical disk and marked that block as invalid. If the controller encountered an unrecoverable medium error on a source physical disk during a rebuild or reconfigure operation, it will also puncture the corresponding block on the target physical disk. The invalid block will be cleared on a write operation. Back up your data.
2282	Hot spare SMART polling failed	Failure	The controller firmware attempted a SMART polling on the hot spare but was unable to complete it. The controller has lost communication with the hot spare. Check the health of the disk assigned as a hot spare. You may need to replace the disk and reassign the hot spare. Make sure the cables are securely attached.
2289	Multi-bit ECC error	Failure	An error involving multiple bits has been encountered during a read or write operation. An error involving multiple bits indicates data loss. Replace the dual in-line memory module (DIMM) The DIMM is a part of the controller battery pack. See the hardware documentation for information on replacing the DIMM. You may need to restore data from back up.
2299	Bad PHY %1	Failure	There is a problem with a physical connection or PHY. The %1 is a text string which varies depending on the situation. Contact Avaya Support.
2307	Bad block table is full. Unable to log block %1	Failure	The bad block table is used for remapping bad disk blocks. When the table is full, bad disk blocks can no longer be remapped, disk errors can no longer be corrected, and data loss occurs. The %1 is a text string which varies depending on the situation. Replace the disk which is generating this alert. If necessary, restore your data from back up.
2320	Single-bit ECC error	Failure	The DIMM is malfunctioning. Data loss or data corruption may be imminent. Replace the DIMM immediately to avoid data or loss data corruption. The DIMM is a part of the controller battery pack. See your hardware documentation for information on replacing the DIMM.

Event ID	Description	Severity	Cause and Action
2321	Single-bit ECC error	Failure	The DIMM is malfunctioning. Data loss or data corruption is imminent. No further alerts will be generated. Replace the DIMM immediately. The DIMM is a part of the controller battery pack. See your hardware documentation for information on replacing the DIMM.
2340	The BGI completed with uncorrectable errors	Failure	The BGI task encountered errors that cannot be corrected. The virtual disk contains physical disks that have unusable disk space or disk errors that cannot be corrected. Replace the physical disk that contains the disk errors. Review other alert messages to identify the physical disk that has errors. If the virtual disk is redundant, you can replace the physical disk and continue using the virtual disk. If the virtual disk is non-redundant, you may need to recreate the virtual disk after replacing the physical disk. Run Check Consistency to check the data after replacing the disk.
2347	The rebuild failed due to errors on the source physical disk	Failure	You are attempting to rebuild data that resides on a defective disk. Replace the source disk and restore from back up.
2348	The rebuild failed due to errors on the target physical disk	Failure	You are attempting to rebuild data on a disk that is defective. Replace the target disk. If a rebuild does not automatically start after replacing the disk, initiate the Rebuild task. You may need to assign the new disk as a hot spare to initiate the rebuild.
2349	A bad disk block could not be reassigned during a write operation	Failure	A write operation could not complete because the disk contains bad disk blocks that could not be reassigned. Data loss may have occurred and data redundancy may also be lost. Replace the disk.
2350	There was an unrecoverable disk media error during the rebuild.	Failure	The rebuild encountered an unrecoverable disk media error. Replace the disk.

Index