Avaya Aura® System Manager 6.2

Release Notes

March 2012

Issue: 1.1

September 6, 2012

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 might be incorporated in future releases.

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 the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product, while under warranty, is available through the Avaya Support Web site: http://support.avaya.com

License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE

http://support.avaya.com/LicenseInfo/("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

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 the Avaya Support Web site:

http://support.avaya.com/ThirdPartyLicense/

Preventing toll fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com

Trademarks

Avaya and the Avaya logo are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions. All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://support.avaya.com

Avaya support

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

Table of Contents

Introduction

This Release Note gives you information about Avaya Aura® System Manager 6.2 application and the supported documentation. The Appendix sections describe the procedure for changing IP address or host name, changing date and time configuration, the Cold standby procedure, how to schedule a data backup and restore a backup script for Avaya Aura ® System Manager and Avaya Aura ® System Platform HA mechanism, and how to reset a user password. This Release Note also contains information about known issues and the possible workarounds.

Note - For information on installing and upgrading to System Manager 6.2, see *Avaya Aura System Manager 6.2 Install/Upgrade guides and Administrator Guide* on the Avaya Support Web site at http://support.avaya.com

Avaya delivers System Manager 6.2 in the form of a template. You must deploy the template as a virtual appliance on Avaya Aura® System Platform 6.2.0.0.27.

Product Support Notices

Some product changes are documented as Product Support Notices (PSN). The PSN number defines the related document.

To read a PSN description online:

1. Go to the Avaya Support Web site at http://support.avaya.com.
2. On the main menu, click **Downloads and Documents**.
3. In the **Enter Your Product Here field**, enter System Manager or select **Avaya Aura® System Manager** from the list.
4. In the **Choose Release** field, click **6.2.x**.
5. Click **Documents**.
6. Check **Product Support Notices**.
7. Click **Enter**.
8. To open a specific PSN, click the PSN title link.

System Manager Software

System Manager Installation and Download

#	Action	Notes
1.	Download the System Platform 6.2.0.0.27 ISO image and patch 1 from the Avaya PLDS Web site.	Verify that the md5sum for the downloaded ISO image matches the number on the Avaya PLDS Web site.
2.	Download the System Manager 6.2 IU info on PLDS Download Name: Avaya Aura System Manager 6.2 ISO File Name: System_Manager_06_02.iso	PLDS download ID: SMGR62GA001 md5Sum: bd7c95e4d86698251af3ee5d7c32c6a3
3.	Deploy the System Manager 6.2 template	You must install the System Manager 6.2 template on System Platform 6.2.0.0.27. **Note:** *Please refer "**Installing a solution template**" section of* ***Implementing Avaya Aura® 2 System Manager R6.2*** *guide*

Note: System Manager 6.2 is a full ISO image. When you download System Manager 6.2 from Product Licensing and Delivery System (PLDS), copy the software to a DVD as an ISO image. You must install System Manager 6.2 on System Platform 6.2.0.0.27 through CDOM Virtual Machine Solution Template before installing System Manager 6.2

What's New in this Release

Please refer 6.2 **Administering Avaya Aura® System Manager** Section "What is new in this release".

Must Read for a fresh installation or an upgrade

.

1. **User with end user role cannot log on to System Manager Release 6.2.x Release.**
2. **Backup and Restore through System Platform.**

   A backup data obtained from System Platform should be restored on same version of System Platform.
3. **Backup and Restore through System Manger.**

   It is recommended that backup data obtained from System Manager should be restored on same version of System Manager.
4. **Upgrade System Platform before the System Manager upgrade**

   You must deploy System Manager 6.2 as a virtual appliance on System Platform 6.2 0.0.27. To upgrade System Manager, you must first upgrade System Platform and install System Platform patches, if any, and upgrade System Manager 6.2.
5. **Reboot the system after upgrading to 6.2**

   System Manager 6.2 includes some kernel updates. To ensure that the updated kernel runs in memory, you *must reboot the system* from System Platform or through the System Manager command line interface (CLI).
6. **Verify the System Manager Release version**

   After successful installation of System Manager 6.2, to verify the release of the installed System Manager click **About** on the top-right corner of the Home page or execute the **swversion** command through the CLI. The system displays the version information in the following format:

   System Manager 6.2.0 [Build No. - 6.2.0.0.15669-6.2.12.9] Software Update Revision No: 6.2.12.1.1822
7. **Use FQDN while accessing System Manager**

   Avaya recommends the use of Fully Qualified Domain Name (FQDN) instead of the IP address to gain access to System Manager 6.2.
8. **Admin User / Non Admin Users password change**

   For Avaya Unified Communication Management to authenticate the administrator login ID “admin”, enter the password **admin123**.

   - For Avaya Aura® System Manager to authenticate the administrator login ID “admin”, you can use the following password:
   - For fresh installation, the password is set to **admin123.**
   - For upgrades from System Manager Release 6.1 to System Manager Release 6.2, the administrator password remains the same.
   - For upgrades from System Manager Release 6.0 to System Manager 6.2, the administrator password is reset to **admin123**.
   - The password of other administrative users is reset to the user ID of the user after the upgrade. For example, the password for dsmith@avaya.com is set to dsmith@avaya.com

- When you promote End user to Administrator, the password for the End user will reset to the user’s Login Name.

9. **Change password**

   To change the **admin** password, on the dashboard, click **Users > Administrators > Avaya Unified Communication Management**. On the Avaya Unified Communication Management page, click **User Services** > **Password**.

10. **Password policy and aging for admin user account**

    To verify the password policy and aging for **admin**, use the Avaya Unified Communication Management page. On the dashboard, click **Users** > **Administrators** > **Avaya Unified Communication Management**. On the Avaya Unified Communication Management page, click **Security** > **Policies**.

11. **External authentication configuration**

    If you upgrade directly to System Manager 6.2 from an earlier release, and if you have configured the earlier release for an external authentication, such as LDAP and RADIUS, prior to the upgrade, you must manually recon figure external authentication server details on System Manager 6.2 after the system completes the upgrade. To reconfigure System Manager, click **Users** > **Administrators** > **Avaya Unified Communication Management**. On the Avaya Unified Communication Management page, click **User Services** > **External Authentication** to modify external identity repositories.

12. **Log-in warning banner**

    If you want to upgrade directly to System Manager 6.2 from an earlier release, and if you have configured for the legal notice, you must manually reconfigure the log-in warning banner content on System Manager6.2 after the system completes the upgrade. To reconfigure, on the Avaya Unified Communication Management page, select **Security** > **Policies** and click **Edit** to modify the log-in warning banner in the **Security Settings** section.

13. **No authentication required for user bulk export**

    While running the bulk export utility for bulk export users, do not specify the user name or password.

14. **Backup and Restore through System Platform**

    A backup of System Manager obtained after performing a backup on a particular version of System Platform, cannot be used to restore to an older version of System Platform.

15. **Administer CS1000**

    System Manager 6.2 is integrated with Unified Communications Management (UCM) 7.5. After you install the System Manager template, UCM and System Manager reside on the same server. You can log in to System Manager or UCM using the Single-Sign-On page. For more information on UCM and how to administer CS1000 using System Manager, see Unified Communications Management Common Services Fundamentals and Subscriber Manager Fundamental version 7.5 at http://support.avaya.com.

16. **IP Sync on CM**

While synching the IP interfaces from CM, System Manager shall ignore the IP interfaces if node name is not configured. Even though the Node Name field is not required on the CM SAT, it is needed to administer the IP Interface in other forms. So System Manager is only synching those IP Interfaces that have the node name field populated.

17. **CM Roles after Fresh & upgrade**

If you have upgraded from an earlier Release of System Manager then “Communication System Management Admin” and “Communication System Management Viewer” roles are no longer default roles. They retain the same role assignments but are now non-default roles which can be changed by the user.

On a fresh install of 6.2 the “Communication System Management Admin” and “Communication System Management Viewer” roles would not be available.

18. **Dialplan change on CM requires Full Sync**

If there is a change in any of the below objects on CM then it is required to do a full initialization sync of this CM in System Manager for proper operation.

system-param features
system-param cdr
system-param cust
system-param spec
system-param security
system-param country-options
system-param maintenance
dialplan
cabinet
board

19. **Messaging & Discovery jobs after upgrade**

Messaging & Discovery (Collect Inventory) jobs scheduled in earlier releases will fail after upgrade to 6.2 GA build.

Steps to get these jobs working:

Disable the Messaging and Discovery jobs that are failing after upgrade.

Create new jobs for Messaging and Discovery (Collect Inventory) from Inventory in System Manager 6.2.

20. **RAID Controller Battery Check**

Before proceeding the Installation / Upgrade please check the RAID Controller Battery state. When the RAID Controller Battery is depleted (or otherwise compromised), the Disk Cache policy is set to “WriteThrough” therefore slowing down overall I/O operations. This may impact on Installation / Upgrade process.

21. **Preferred Handle field in CM Endpoint Profile for the Communication Profile of a User**

Preferred Handle field provides numeric only handles, SIP or non SIP, that are administered for a user. The Preferred Handle field is optional. If the SIP entity is of Communication Manager Type, Session Manager uses the Preferred Handle field in CM Endpoint profile.

By default, for a SIP station, Communication Manager uses the extension number as the Phone Number entry on an OPS station-mapping table. If your enterprise dial plan has SIP handles that are different from the CM extension, then use the Preferred Handle field to change the phone number entry on the OPS station-mapping table on the Communication Manager.

To modify the phone number entry, the Communication Address in System Manager should have a SIP handle. In the CM Endpoint Communication Profile, set the Preferred Handle field to the SIP handle format. After you click Commit System Manager sets the Phone Number field in the OPS station-mapping table on CM to the SIP handle format.

If you do not need this feature then set the Preferred Handle value to “None”. By default, the Preferred Handle field is set to None. **E.164 is not a valid value for Preferred Handle in this release.**

22. **Scheduling Jobs**

    If a scheduled job has completed all its occurrences then do not edit the job and enable it again. Instead, it is recommended that you create a new scheduler job for performing the same task. If we enable a job which has completed all it occurrences then after an upgrade the job will be in a disabled state and will have to be enabled again manually.

Prerequisites

- To deploy System Manager 6.2 you must install System Platform 6.2.0.0.27.
- Before installing System Manager 6.2, you must take a backup of the system and store the backup on an external device.
- If you upgrade System Manager from an earlier release and if the System Platform upgrade is required, you must upgrade System Platform before you upgrade System Manager.

Supported hardware

- IBM x3550m2
- HP ProLiant DL360 G7 2CPU MID4
- Dell™ PowerEdge™ R610 2CPU MID2

Software dependencies

Software	Version	Note
Postgres	9.0.2	The Postgres version 9.0.2 is used as the System Manager database Automatic String to Byte conversion is not supported in 9.0.2. For more information, see http://www.postgresql.org/docs/9.0/static/release-9-0.html for changes
CentOS	5.4 64 bit	CentOS-5.4 64-bit is used as the base OS for the System Manager template.
JDK	Version 6 Update22 32-bit	JDK6 update22 32-bit is used.
JBoss	4.2.3	Jboss is used as the application server for the System Manager software.

Installation note

See the Avaya Support Web site at **http://support.avaya.com** for the following:

- System Manager 6.2 installation and configuration information in the **Implementing Avaya Aura® System Manager 6.2** guide
- System Manager 6.2 upgrades information in the **Upgrading Avaya Aura® System Manager to 6.2** guide
- Installation and upgrades, product support, and service packs for earlier releases of System Manager 6.2.

Supported upgrades

Note:

- Please refer the document "Upgrading Avaya Aura® System Manager to 6.2" to upgrade older System Manager Release to System Manager 6.2 Release.

Known problems

This release includes the following known problems in System Manager:

Table 8: Known problems in System Manager 6.2

Reference ID	Description	Keyword	Workaround
wi00871848	While trying to import a user from LDAP or AD with an attribute value "localizedname" and when to synch user with LDAP or AD, system Manager throws error.	Directory synchronization	No workaround available
wi00909208	The status of the logged out user remains Online in System Manager	User Profile Management	No workaround available
wi00925951	Refresh button in the Serviceability agent page does not refresh	SNMP	No workaround available
wi00926769	Non- user friendly error seen on the Log Harvesting UI when you click on searched results panel.	Log Harvesting	No workaround available
wi00926818	Incase of direct e-token access to System Manager, that is, without Axeda & SAL Gateway, Services Denied to Regular users after gaining Access to the system with e-token.	Trust Management	No workaround available
wi00938737	Roles assigned to the user are removed when you call 'changePassword' method	User Profile Management	No workaround available
wi00943573	The Search option in Log harvesting retrieves wrong data	Log Harvesting	No workaround available
wi00947797	The Search option in Log harvesting retrieves wrong data when a user searches with a wildcard entry	Log Harvesting	No workaround available
wi00948629	System Manager logs the user out off the interface even when the user selects the "stay on page".	Common Console	No workaround available
wi00951216	The alarm exported into the excel sheet do not show up in the correct order.	Alarming	No workaround available
wi00962948	Stopping an On-demand job does not stop the job.	Scheduler	No workaround available

wi00963647	AgedAlarmPurgeRule and ClearedAlarmPurgeRule are not able to delete backdated alarms	Element Manager	No workaround available
wi00966119	The Previously assigned roles are lost after a user assign a new role from "**More Actions**" > **Assign Role**	User Profile Management	No workaround available
wi00853849	The "Backup Time" column on the BackupRestore screen displays the Time even when the backup state is PLANNED/RUNNING	Element Manager	No workaround available
wi00876360	The Help links on "-Home / Services / Configurations / Settings-" welcome matt and sub-links should point to relevant help pages	Configuration Management	No workaround available
wi00896448	On the Elements page all editable buttons are displayed in disabled mode if a user revisits Dashboard > **Users** > **Administrators** > **Elements** > **Subscriber Manager Element**	Unified Communication Manager	No workaround available
wi00903838	Old CA certificates are (from Dashboard > Elements > Inventory > System Manager > More Actions > Configure Trusted Certificates) not deleted after upgrade.	Trust Management	No workaround available
wi00907679	Admin user is able to change permissions of Default admin user	User Profile Management	No workaround available
wi00927568	Schedule Later section is enabled at Dashboard > Elements > Inventory > Manage Elements > More Actions > Import Screen by default.	Configuration Management	No workaround available
wi00964122	Select button in table for User Profile > Membership - Assign Roles does not consider the previous page selection.	User Profile Management	No workaround available

wi00966176	Delete' button appears disabled, when multiple user records are selected in User Profile Screen	User Profile Management	No workaround available
wi00973943	Date and Time Configuration and IP-FQDN change may not work the second time, when we change from System Platform	Configuration Management	Login to System Manager using ssh, change user to root. Run command: $ umount /media/netchng
wi00967910	Issues related to adding Messaging System in Manage Elements – no validation checks for Messaging type and version, improper log if sync fails due to wrong version of CMM 6.2.	Messaging System	Do not change the Messaging type after adding it in Manage Elements. Make sure to give correct Messaging System Versions in Manage Elements that are supported by System Manager.
wi00968077	In Upgrade Management after the successful upgrade of the device, the device reboots & System Manager receives the warmstart alarm. But the version of device is not updated automatically on System Manager GUI.	Upgrade Management	Run Status job or click on RUNNING state to update the device status.
wi00967764	In Upgrade Management software library, SCP transfer fails when specifying windows style (D:\ABGup\fw\) server path for SCP server running on Windows.	Upgrade Management	Use linux style server path (/cygdrive/d/ABGup/fw/).
wi00967912	When an endpoint is added in CM endpoint communication profile with override endpoint name set to true and with a name which has more than 27 characters, then when this name is changed after doing change station-extension on CM we see difference in the name that appears on CM SAT and the one which appears in System Manager after incremental sync.	Communication Manager Synchronization, Override Endpoint Name	No workaround available
wi00956765	Endpoint button assignments get lost if endpoint editor is launched for editing and there are any button assignment issues due to which the edit fails.	Endpoint Communication Profile, Communication Manager	Redo all the button assignments again in edit endpoint editor screen.
wi00968773	Endpoint User association gets removed if synchronization is run after executing change extension-station from CM SAT (outside System Manager).	Endpoint Communication Profile, Communication Manager	Redo the Endpoint communication profile for the user.

wi00969861	Deletion of CM (with large number of endpoints, say more than 10-15K) from System Manager Database is slow.	Communication Manager	Wait for 15 – 20 minutes for CM to be deleted from the System Manager Database.
wi00969495	Messaging Maintenance Job is not created after System Manager upgrade from 6.1 SP6 to 6.2 GA build	Messaging System	Add a new Messaging System with any dummy details (do not use "dummy" as the Messaging system name, any other name will do). The job is created. Then delete this dummy messaging system.
wi00963655	Last operation column is not getting updated properly on B5800 page if you schedule a sync job of 'system configuration and user' for large number of B5800 devices	B5800 Branch Gateway	No workaround available
wi00962074	Incorrect status on B5800 Backup and Restore page for backup job run for large number of B5800 devices	B5800 Branch Gateway	No workaround available
wi00969321	Display station shows SIP trunk as blank on CM SAT when the trunk is changed from endpoint editor when assigning preferred handle at the same time.	Endpoint Communication Profile, Communication Manager, Preferred Handle	Do not assign preferred handle while changing SIP trunk in Manage Users if there is no need for it.
wi00969349	Assigning preferred handle always changes the first off pbx station mapping entry irrespective of the application type.	Endpoint Communication Profile, Communication Manager, Preferred Handle	No workaround available
wi00962283	B5800 Upgrade Manager UI issues – HTTPS is listed as a protocol to download file when it should not be listed. The HTTPS protocol is currently used in System Manager to copy the file from S/W library to the device and not for download to library from PLDS/ Software repository. After starting download of file from PLDS/ repository, leave the File Download Manager page for 10-15 minutes. Then refresh the Device tree. The whole tree vanishes.	Upgrade Management	To see the tree again, you need to select the library again.

wi00966530	Proper logs for error conditions are missing in Upgrade management.	Upgrade Management	No workaround available
wi00967906	Edit User having Messaging communication profile fails with error 'attribute Mail is invalid' if we go to Messaging editor	Messaging System, Messaging Communication Profile	When you go to subscriber editor, go to subscriber tab & clear 'Email Handle' field.
wi00963731	Internal error when we commit Software library with Server path set as "/"	Upgrade Management	Use path other than just "/".
wi00964586	Change in location number in Feature Options does not take effect when using Endpoint Editor under User Management	Endpoint Communication Profile, Communication Manager,	Change location value from Manage Endpoint Feature option screen instead.
wi00872272	If you open multiple tabs for same function (like say two tabs for Communication Manager) and try to do similar operations in both, you can get internal errors.	Communication Manager	Use one tab for a function.
wi00963376	After analyze, available/entitled versions shown as "N/A" if device already on latest firmware version.	Upgrade Management	No workaround available
wi00963837	Delete software library files from System Manager fails in a scenario where if the download operation has failed, then when the next download is successful, there will be 2 entries in System Manager database. One for failure and other one for success. Due to this the library deletion fails.	Upgrade Management	No workaround available
wi00975303	Incremental Sync fails for Communication Manager if multiple locations is disabled after it was previously enabled and synced with System Manager.	Communication Manager	Run Initialization Sync
wi00976193	Notify sync does not work for Duplex CM added with Virtual IP.	Communication Manager	Need to add duplex CM with Active Server (as Node IP) & Standby Server IP (as alternate IP) in Manage Elements. If the CM has been discovered, then user needs to change the CM node IP

			from Virtual to Active Server IP for CM Notify Sync feature to work.
wi00978656	If we have scheduled jobs with frequency as monthly then it may cause upgrades to fail	Scheduler	Change the frequency of the Monthly Jobs to weekly and then try the upgrade
wi00975891	Error displaying on the System Manger dashboard "Some internal error has occurred in the service." If we click on Services > Backup Restore page	Backup	Refresh the screen
wi00981037	Trust Management is not checking for expired identity certificates	Trust Management	No workaround available

Technical support

Support for System Manager 6.2 is available through Avaya Technical Support.

In case of issues with System Manager 6.2, you can:

- Retry the action. Carefully follow the instructions in the printed or online documentation.
- See the documentation that ships with your hardware for maintenance or hardware-related problems.
- Note the sequence of events that led to the problem and the exact messages that the system displays. See the troubleshooting section of the Avaya product documentation.

If you continue to have problems, contact Avaya Technical Support using one of the following methods:

- Log in to the Avaya Support Web site at **http://support.avaya.com**.
- Call or send a fax message to Avaya Support on one of the telephone numbers in the Support Directory listings on the Avaya Support Web site.

Using Avaya Global Services Escalation Management, you can escalate urgent service issues. For more information, see the list of Escalation Contacts on the Avaya Support Web site.

Before contacting Avaya Support, keep the following information handy:

- Problem description.
- Detailed steps to reproduce the problem, if any.
- The release version in which the issue occurs.

Note:

To know the release version and build number, log in to System Manager and click **About** on the dashboard.

- The status of the System Manager software. If the software is an upgrade, provide the current release number.
- The installation log files.
    a. System Manager JBoss server log file available at ***$JBOSS_HOME/server/avmgmt/log/server.log***.
- Additional System Manager Logs available in the ***$AVAYA_LOG/mgmt*** location***.***

Contact support tasks

Avaya Support might request for e-mail notification files for analysis of your application and the application environment.

For information about patches and product updates, see the Avaya Support Web site at http://support.avaya.com

Appendix A: Changing the IP address or host name

After you deploy System Manager, you can change the IP address or the host name of the computer on which System Manager is running. Use System Platform Web Console to effect the change.

Prerequisites

- Ensure that System Manager is installed on the system and is accessible. You can verify this by accessing the System Manager Web user interface.
- Ensure that all extension packs are successfully deployed:
  a. Log in to System Manager as an administrator using the login **admin**.
  b. On the dashboard, click **Services > Configurations**.
  c. In the left navigation pane, click **Extension Packs**.
  d. Verify that the status of the extension pack data is in the Confirmed state.
- After installing System Manager, if you modified any configuration settings on the Settings page, you must make these changes again after you change the IP address or the host name. Note down the changes.
- Ensure that you have performed a manual backup by using the remote backup facility of System Manager Element Manager and data is backed up successfully. For more information on backup, see "Backing up System Platform" in Upgrading Avaya Aura® System Manager to 6.2

  Note: Copy the backup to a remote computer or to an external storage device, such as a CD-ROM or a DVD.

Changing the IP address and FQDN of System Manager

Changing the IP address of System Manager

1. Go to the System Platform Web Console at https://<C-dom IPAddress>/webconsole.
2. Log in as an administrator using the login **admin**.
3. Click **Server Management > Network Configuration.**
4. On the Network Configuration page, click **Template Network Configuration**.
5. Modify the following fields in the **Template Network Configuration** section:
   a. Change the IP address to System Manager IP Address.
   b. Change Netmask under Domain Network Interface for Bridge avpublic.

   c. Change the server to a different subnet with a new default gateway address.

   d. Change the default gateway in the General Network Settings section.

6. Click **Save**. The system displays the following confirmation message: “Changing network setting may require you to log in again into Avaya Aura System Platform webconsole. Are you sure? “
7. After you confirm the status message, the system displays: Processing your request, please wait…. Once the system completes the processing and network change, the system displays the following status message: Settings updated successfully.
8. Verify that the System Manager Web Console is accessible.

If you configured the SAL Gateway to receive SNMP traps from System Manager, then perform the following tasks from the System Platform Administration user interface:

1. Go to System Platform Web Console at https://<C-dom IPAddress>/webconsole.
2. Click **Server Management**.
3. Click **SAL Gateway Management**.
4. Click **Launch SAL Gateway Management Portal**.
5. On the Avaya SAL Gateway log-in page, log in as an administrator using your admin privileges.
6. Click **Managed Element**.
7. Click System Manager Hostname in the **Host Name** column displayed in the Managed Elements Found table.
   a. The system displays the Managed Element Configuration page.
8. Click **Edit** and modify the **Host name** field to the new host name.
9. Modify the **IP Address** to the new IP address.

Changing the host name of System Manager

1. Go to System Platform Web Console at https://<C-dom IPAddress>/webconsole.
2. Log in as an administrator using the login **admin**.
3. Click **Server Management.**
4. Click **Network Configuration**.
5. On the Network Configuration page, click **Template Network Configuration**.
6. On the Template Network Configuration page, in the **Change the Host name marked as Hostname:**
   a. field in the **Global Template Network Configuration** section, enter the System Manager

b. Fully Qualified Host name for the System Manager.

Note: Fully qualified domain name should be as "Hostname.SecondLevelDomain.TopLevelDomain"
If Fully qualified domain name does not contain top-level domain, hostname change will be successful, but due to failure in configuration the System Manager local-login page will come up instead of normal login page.

7. Click **Save**. The system displays the following confirmation message: Changing network settings may require you to log in again into webconsole. Are you sure?
8. After you save the changes, the system displays: Processing your request, please wait…. Once the system completes the processing and network changes, the system displays the following status message: Settings updated successfully.
9. Wait for the network change to take effect and then verify that System Manager Web Console is accessible.

If the SAL Gateway is configured to receive SNMP traps from System Manager, then perform the following tasks from the System Platform Administration UI:

1. Go to System Platform Web Console at https://<C-dom IPAddress>/webconsole.
2. Click **Server Management**.
3. Click **SAL Gateway Management**.
4. Click **Launch SAL Gateway Management Portal**. The system displays a new window.
5. Log in as an administrator using **admin** privileges.
6. Click **Managed Element**.
7. Click System Manager Hostname in the **Host Name** column displayed in the Managed Elements Found table. The system displays the Managed Element Configuration page.
8. Click **Edit** and modify the Host name field to the new host name.
9. Modify the **IP Address** to the new IP address.

Changing the System Manager IP address and FQDN referenced in the managed elements

Changing System Manager IP referenced in managed elements

After you change the IP address of System Manager, perform the following procedure to change the IP address of Managed Elements:

1. If the Managed Elements feature uses the JNDI lookup to communicate with System Manager, ensure that all managed elements refer to the new System Manager IP address.
2. The change in the IP address of System Manager affects License Management. Ensure that:

- The adopting product application recreates the License Manager object with the new IP address.
- You redo all license acquisitions after the adopting product application recreates the object.

Changing the System Manager Hostname referenced in managed elements

If you changed the host name of managed elements, you must also make the following change:

1. If the Managed Elements feature uses the JNDI lookup to communicate with System Manager, ensure that all managed elements refer to the new System Manager Host name.

Perform the following steps to make changes in the SAL Agent from the CLI.

1. Edit the host name of the managed element to the new host name in the following files:
   - **$SPIRIT_HOME/config/agent/SPIRITAgent_1_0_DataTransportConfig_orig.xml**
   - **$SPIRIT_HOME/config/agent/SPIRITAgent_1_0_BaseAgentConfig_orig.xml**
   - **$SPIRIT_HOME/config/agent/SPIRITAgent_1_0_SpiritComponentConfig_orig.xml**

   where $SPIRIT_HOME is the base location of the SAL agent deployment on the managed element.
2. Restart the SAL Agent using the following command:

   # service spiritAgent restart

The change in the host name impacts License Management. Ensure that:

1. The adopting product application recreates the License Manager object with the new IP address.
2. You redo all license acquisitions after the adopting product application recreates the object.

The change in the host name impacts the Data Replication Service (DRS) client application. Perform the following steps to make changes in the DRS client application:

1. Edit all occurrences of the new System Manager host name in the following files:
   - **$SYM_HOME/WEB-INF/classes/symmetric.properties**
   - **$DRS_HOME/conf/drsClientInstall.properties**
2. Restart the DRS client.

Changing the IP address and FQDN of managed elements

For information on changing the IP address and FQDN of the managed elements, see the product documentation of the respective managed element.

Changing the IP address and FQDN of managed element in System Manager

Procedure in System Manager

If the identity certificates of the clients contain the IP address of the client computer, ensure that the certificates are reinitialized as per the changed IP address of the client computer. This prevents host name verification failure during communication between the client and the service.

If Managed Elements is registered with System Manager using an IP address, then:

1. Log in to System Manager as an administrator using the login **admin**.
2. On the dashboard, click **Elements** > **Inventory**.
3. In the left navigation pane, click **Manage Elements**.
4. On the Manage Elements page, select the registered element and click **Edit**.
5. Update the values for **Node** in the **Application** section and **Host** in the **Access Point** section.

Procedure in Managed Elements

Use the following procedure to make changes in the SAL Agent from the command line interface (CLI):

1. Change all occurrences of the old IP address of Managed Elements to the new IP address in the following file:

   $SPIRIT_HOME/config/agent/SPIRITAgent_1_0_supportedproducts_orig.xml

2. Restart the SAL Agent using the following command:

   ```
   # service spiritAgent restart
   ```

Changing FQDN of managed element in System Manager

Procedure in System Manager

If the identity certificates of the clients contain the host name of the client computer, ensure that the certificates are reinitialized as per the changed host name of the client computer.

If Managed Elements is registered with System Manager using a host name, then:

1. Log in to System Manager as an administrator using the login **admin**.
2. On the dashboard, click **Elements** > **Inventory**.
3. Click **Manage Elements**.
4. On the Manage Elements page, select the registered element and click **Edit**.
5. Update the values for **Node** in the **Application** section and **Host** in the **Access Point** section.

Procedure in Managed Elements

Perform these steps to make changes in the SAL Agent from the CLI:

1. Edit all occurrences of the IP address of managed elements in the following file:

   $SPIRIT_HOME/config/agent/SPIRITAgent_1_0_supportedproducts_orig.xml

2. Restart the SAL Agent using the following command:

   ```
   # service spiritAgent restart
   ```

This section describes the changes you must make to the DRS Client. You can opt for any of the procedures provided here.

- Re-register the node in case of Session Manager:

    1. Stop the client service that hosts the DRS client application.
    2. Remove the client node from the DRS GUI.
    3. From the CLI, run the following script:

        # sh /opt/Avaya/bin/initTM

- Reconfigure the node in case of Presence Services:

    1. Stop the client service that hosts the DRS client application.
    2. Remove the client node from the DRS GUI.
    3. From the CLI, run the following script:

        # sh $DRS_HOME/bin/start_aggregation.sh

    4. From the CLI, run the following script:

        # sh $DRS_HOME/bin/get_initial_load.sh

    5. Start the client service that hosts the DRS client application.

Note:

Log in to the System Manager Web Console and verify the functionality. If the system is unstable, use the Cold stand-by procedure to restore the system to the state prior to the change. For Cold standby procedures, see **Appendix C**.

Appendix B: Changing the date and time configuration

You can change the date, time, and time zone of System Manager from System Platform Web Console.

Prerequisites

- Ensure that System Manager is installed on the system and accessible.

Changing the time zone on the computer on which System Manager is running

1. Go to System Platform Web Console at https://<C-dom IPAddress>/webconsole.
2. Log in as an administrator using the login **admin**.
3. Click **Server Management**.
4. Click **Date/Time Configuration**.
5. Select a **time zone** from the list in the time zones section.
6. Click **Set Time Zone** and click **OK** to confirm the change. The system displays the following status message: Processing your request, please wait.... Once the system completes the operation, the system displays the following status message: Time zone has been changed to <new time zone>.
7. After the operation, restart the JBoss service by performing the following steps:
   a. Log in to System Manager from the CLI.
   b. Use the service JBoss restart command to restart JBoss.
   c. Wait till the system displays the System Manager log-in page again.

Changing the date or time on the computer on which System Manager is running

1. Go to System Platform Web Console at https://<C-dom IPAddress>/webconsole.
2. Log in as an administrator using the login **admin**.
3. Click **Server Management**.
4. Click **Date/Time Configuration**.
5. Ensure that the Network Time protocol daemon (ntpd) is not running.
6. Click the text box that contains the date and time information. The system displays a pop-up calendar.
7. Enter the new time value in the **Time** input field.
8. Select a date value in the calendar.
9. Click **Apply to proceed** with the changes.
10. Click **Save** Date and Time and click **OK** to confirm the change. The system restarts.
11. Wait for System Platform to redirect you to the log-in page - Verifying changes in the date and time configuration
12. Log in to the system running System Manager from the CLI.
13. Type **date** and press **Enter**. You can view the updated date, time, and time zone values.
14. After verifying the updated values, type **Exit** and press **Enter**.

Appendix C: Cold standby procedure

Introduction

The System Manager server in the Cold standby mode acts as a failover when the main server on which System Manager is running fails. This section covers the Cold standby failover process for the System Manager application deployed on System Platform. The process is described with the example of two nodes: an Active node and a Cold standby node. Node A is the primary machine that is active. Node B is the Cold standby server. You must implement the Cold standby procedure in a scenario where Node A fails and the application must failover to Node B.

Prerequisites

Ensure that:

- Node A and Node B are installed on identical servers. The system supports the following servers: Dell™ PowerEdge™ R610 Server and HP Proliant DL360 G7.
- Node A (Active Node) and Node B (Cold standby Server) have the same IP address and host name. Ensure that when the Active Node is running, the Cold standby server is turned off.
- The System Manager 6.2 template is deployed on Node A and Node B. For the procedure to install the template, see **Implementing Avaya Aura® System Manager 6.2**
- The system date is identical on both the nodes.
- Regular backups of the System Manager database of Node A are available. To create these backups, use the Remote backup facility of System Manager Element Manager or create the backups from System Platform Web Console. The backups are necessary so that the latest snapshot of the System Manager database is available in case you need to implement the Cold standby procedure. Retain the backup of the database on a remote node or an external storage device, such as a CD-ROM or DVD. Use the backup to restore the database on Node B when Node A fails. For the procedure to schedule a backup on the System Manager Node, see **Appendix D**.
- When you implement the Avaya Aura® System Manager Cold standby procedure on a different computer, the system does not recognize the previously installed license file as the MAC address changes for the new computer. Use the following workaround or alternative remediation:

  1. The Avaya Business Partner or services technician must generate a new license file for products that are licensed using WebLM and were installed prior to performing Cold standby. Ensure that this new license file is generated from PLDS with the same count and the new MAC address.
  2. Copy the newly generated license file where System Manager is deployed.
  3. Obtain access to the System Manager command line interface (CLI).
  4. Stop the JBoss server using the following command:

     # service jboss stop

5. Delete the unwanted license file with the file extension in xml from the following location:

   # $JBOSS_HOME/server/avmgmt/deploy/WebLM.ear/WebLM.war/licenses

6. To confirm which license file to delete, open the license (.xml) file in a vi editor and look for the <Name> tag within the <Product> element. Verify that the name of the product is similar to the newly generated product name.

7. Once confirmed, delete this xml file using the following command:

   # **rm –rf JBOSS_HOME/server/avmgmt/deploy/WebLM.ear/WebLM.war/licenses/<file_name>**

   Where file_name is the name of the license file that to be deleted.

8. Once you delete the license file, start the JBoss server using the following command:

   # service jboss start

   Note: Wait for 5 to 10 minutes for the Jboss service to start.

9. Log in to the System Manager Console with the administrative user name and password.

   a. Click **UI Licenses > Install license**.

   b. Click **Browse** and select the newly **generated license file**.

   c. Click **Install**.

   Note:

   - On SYSTEM MANAGER 6.2, obtain access to Licenses from the System Manager Dashboard and click **Services > Licenses**.

10. Confirm that the system successfully installed the new license file.

11. Perform steps 1 to 10 for each product.

Notes:
For the procedure to perform a backup from System Platform Web Console, see "Backing up System Platform" in **Upgrading Avaya Aura® System Manager to 6.2.**

Cold standby procedure

1. Confirm that Node A is shut down.
2. Turn on Node B.
3. Install all the System Manager patches on Node B that were installed on Node A before you took the last backup on Node A. For example, if you installed patch 1 and patch 2 on System Manager on Node A before the backup, then install patch 1 and patch 2 on Node B before you restore the backup. In case patch 3 is available and not installed on Node A when the backup was taken, install only patch 1 and patch 2 on Node B. Do not install patch 3.
4. Restore the last database backup that was taken from Node A on Node B. For the procedure to restore the back-up on the System Manager node, see **Appendix E**. If the backup was taken from System Platform Web Console,

see “Restoring System Platform” in [Upgrading Avaya Aura® System Manager to 6.2]() to restore the backup from System Platform Web Console.

5. After restoring the database on Node B, you must run the postColdStandBy.sh script on Node B from the location @ **$MGMT_HOME/utils/bin/coldstandby/postColdStandBy.sh**

   Note:

   After restoring and running the **postColdStandBy.sh** script, System Manager on Node B is available for operations.

6. After restoring the database on Node B, run the following steps to retrieve the TM truststore password:
   a. **sh /home/ucmdeploy/quantum/queryDefaultCertInfo.sh**
   b. Restart **jboss**
7. Once the System Manager comes up, run repair on all replica nodes (Session Manager and Presence nodes) to make sure replicas have data consistent with the data restore on System Manager.
   a. Log in to System Manager as an administrator.
   b. Navigate to **Services > Replications** to open the replication page.
   c. Select all replica groups and click **Repair**. The repair time of all nodes depends on the number of nodes and the size of data populated in the System Manager database.

CLI restore for Cold standby

You can also implement the Cold standby procedure to restore the System Manager database using the CLI utility.

CLI utility properties

While performing a restore from the CLI, you might need to modify some of the restore properties related to the current setup. This file contains the properties related to the CLI restore:
$MGMT_HOME/pem/fileRestoreCLIUtility/fileRestoreCLIUtility.properties.

The following table lists the complete set of properties related to the CLI restore:

No.	Property name	Description
1.	version	The version of the current System Manager setup where you must perform the restore. You can determine the value from both the UI and the CLI. To determine the version from the UI: 1. Log in to System Manager. 2. On the dashboard, click **Services > Configurations > Settings > SMGR**. In the **System Manager Properties** section, the value in **Build Version** is the System manager version. To determine the version from the CLI, use the System Manager version string: **$MGMT_HOME/installer_relno.txt**.
2.	db_type	The database type. The default is set to **postgres**. Do not modify the default setting.
3.	db_directory	The location of the database utility installation. The default location is set to **/usr/bin**. Do not modify the default setting.
4.	db_host	The IP or the host name of the database computer, in this case, the computer on which System Manager is running. The default is set to **localhost**. Do not modify the default setting.
5.	db_port	The database server port. The default is set to **5432**. Do not modify the default setting.
6.	db_name	The database name that must be connected for a restore. The default is set to avmgmt. Do not modify the default setting.
7.	db_scpport	The SSH port to connect the database machine. The default is set to 22**.** Do not modify the default setting unless you modify the configuration for the SSH port.
8.	backup_destination	The full path of the directory to be used as a temporary directory for extracting and processing the backup archives. The default is set to **/var/lib/pgsql/backup**. Do not modify the default setting.
9.	backup_name	The full path to the backup archive, including the archive name. For example, if the archive name is **backup.zip** and the path where the archive is present in the directory: **/var/lib/pgsql/backup/manual/** the value of the backup_name property must be **/var/lib/pgsql/backup/manual/backup.zip**.
10.	scp	The location of the backup archive. Specifies whether the backup archive is stored on the local computer on which System Manager is running or a remote computer. The value false means the archive is on a local computer on which System Manager is running, and the value **true** means the archive is on a remote computer. The default is set to **false**.
11	scp_ip	The IP or the host name of the remote server with the backup archive. Use this property when the value of scp is set to **true**.

No.	Property name	Description
12	scp_port	The ssh port used to connect to a remote server with a backup archive. The default is set to 22. Use this property when the value of scp is set to **true**.
13	user	The user performing the restore operation. You can specify any user name.
14	remote_utility_directory	The full path to the directory that has the System Manager utilities required for the restore. The default is set to **/var/lib/pgsql**. Do not modify the default setting.

CLI restore utility procedure

1. Log in to the system on which System Manager is running as a **root** user. If direct access to the system using the user root is disabled, then log in as a **nonroot** user using direct access to the system. Then escalate access privilege restrictions by issuing the **su** command at the server command line interface.
2. Update the **$MGMT_HOME/pem/fileRestoreCLIUtility/fileRestoreCLIUtility.properties** file with the required details. If the backup archive is present on the local system on which System Manager is running and the default values related to the restore are not modified, update the following properties:

   - version
   - backup_name
   - scp (set to false)
   - user

   If the backup is on a remote system and the default values related to the restore are not modified, update the following properties:

   - version
   - backup_name
   - scp (set to true)
   - scp_ip
   - scp_port
   - user

3. Run the following command to move the CLI Restore Utility from the current directory: **$MGMT_HOME/pem/fileRestoreCLIUtility** to the directory that contains the CLI scripts:

   cd $MGMT_HOME/pem/fileRestoreCLIUtility

4. Run the following command from the current directory:

   ```
   ./file_restore.sh $MGMT_HOME/pem/fileRestoreCLIUtility 1
   ```

5. At the system prompt, enter the full path of the backup archive. If the value is not specified in the **RestoreCLIUtility.**properties file, as mentioned in Step 2, then specify the full path to the backup archive. If the value is already specified in the **RestoreCLIUtility.properties** file, then do not specify any value. Press **Enter**.
6. To perform the restore with the backup archive present on a remote computer with scp set to true, at the system prompt, enter the scp user name. Specify the user name for performing Secure Shell (SSH) on the remote computer and obtain permission to gain access to the backup archive. Press **Enter**.
7. To perform the restore with the backup archive present on a remote computer with scp set to true, at the system prompt, enter the password for the scp user. Specify the password of the scp user mentioned in Step 6, and press **Enter**.
8. The system prompts you to enter the database super user name. Specify postgres as the value and press Enter.
9. At the system prompt, enter the password for the database super user. Specify the password of database super user **postgres** and press **Enter**.
10. At the system prompt, enter a choice for overwriting the current database with the one present in the backup archive. Type **y** and press **Enter**.
11. At the system prompt, enter the database application user name. Specify **postgres** as the value and press **Enter**.
12. At the system prompt, enter the password for the database application user. Specify the password of the database application user **postgres** and press **Enter**.

Appendix D: Scheduling a data backup from System Manager Web Console

1. Log in to the System Manager Web interface as an administrator.
2. On the dashboard, click **Services > Backup and Restore.**
3. Click **Backup**.
4. On the **Backup** page, perform one of the following tasks:

- To schedule a local backup:
  a. Click **Local**.
  b. In the **File Name field**, enter the name of the **backup file** that you want to create.
- To schedule a remote backup:
  a. Click **Remote**.
  b. Specify the SCP Server IP, SCP Server port, user name, password, and file name in the respective fields.
- Click **Schedule**.
- On the Schedule Backup page, complete the following fields: **Job Name**, **Task Time**, **Recurrence** and **Range**.
- Click **Commit**.

Notes:

- If the remote backup server is a Windows server then one should give the full directory path where the backup needs to be stored
- During System Manager backup process local LDAP service will be down for 2 minutes approximately so don't perform any operations on System Manager Web interface during this period.

Appendix E: Restoring a backup from System Manager Web Console

1. Log in to the System Manager Web interface as an administrator.
2. On the dashboard, click **Services > Backup and Restore**.
3. Click **Restore**.
4. On the Restore page, perform one of the following steps:
   - To restore data from a local backup:
     a. Click **Local**.
     b. Enter the backup file name in the **File Name** field.
   - To restore data from a remote backup:
     a. Click **Remote**.
     b. Specify the SCP Server IP, SCP Server port, user name, password, and file name in the respective fields.
     c. Click **Restore**.
5. Click Continue on the Restore confirmation page.

Note:

Ensure that the backup and restore is performed on the same System Manager Patch (same Build Number and Software Update Revision Number). Click the **About** link to view information on the System Manager patch.

The system displays the patch information:

System Manager 6.2.0 [Build No. - 6.2.0.0.15669-6.2.12.9] Software Update Revision No: 6.2.12.1.1822

Appendix F: System Manager HA mechanism

Introduction

System Manager uses the failover mechanism provided by System Platform.

System Platform High Availability (HA) implements the Active and Standby mode of failover. The resources, which are virtual machines (VMs), run only on one node. The system continuously mirrors all disk data from the active mode to the standby mode. In case of failure of the active node, the system automatically starts the resources, that is, the system boots the VMs on the standby node.

System Platform HA uses VMs running on active cluster nodes only. This configuration is also known as the Active/Standby mode. All block devices that are part of the DRBD synchronization propagate all changes from the active node to the standby node. Avaya uses a reliable protocol called C - synchronized replication to ensure that the system commits and acknowledges all block changes on the secondary node before continuing. The system immediately replicates all changes that occur on the active node to the secondary node.

The system performs the following actions in the failover scenario:

- Uses heartbeat to detect problems on the active (primary) node by missing heartbeat checks for a defined period of time.
- Assigns the secondary node as a new primary node.
- Sets the DRBD devices as a primary node on a new active node.
- Boots the VMs on the new active node.

The system performs the following actions in the manual switchover scenario:

- Shuts down the VMs on the active node.
- Sets the DRBD devices as the secondary node on the active node.
- Assigns the secondary node as a new primary node and vice versa.
- Sets the DRBD devices as the primary node on a new active node.

The system boots the VMs on a new active node.

Prerequisites

System Platform uses the simplest HA scenario:

Uses two equal nodes with one public network interface card (NIC) and one HA-dedicated NIC, which is used for HA pings and DRBD propagation between the two nodes.

- Uses both NICs as ping paths between cluster nodes and uses the network switch (gateway IP address) as a public ping point. As a result, each node has three ping points. Heartbeat detects the node with more communication paths available and migrates resources into this node.
- Uses the default port for the ping (port 694).
- Uses the Active/Standby configuration, where all resources run on only one node and all resources are migrated.
- Maintains the same IP address for all VMs, for example, CDom and System Manager on the active and standby nodes.
- Uses heartbeat to start the DRBD service on both the nodes.
- For each VM on the selected cluster node, heartbeat starts the DRBD resources of all VMs and then heartbeat starts the VM itself.

The system uses a Domain 0 LVM to synchronize data by DRBD between the cluster nodes. For this resource, the system defines the mounting procedure on an active node.

Performing System Platform-based HA

1. Install System Platform on two computers.
2. Install the System Manager template on one of the computers. Name this computer **preferred**.
3. Connect the computers with a crossover cable on ports eth2. You must do this before you configure HA Failover.
4. Perform all the required checks on the standby node from the Web console. You must do this before you configure HA Failover. The Standby Web console is not accessible after you configure HA Failover.
5. Configure System Platform HA Failover from the preferred node Web console.
6. Ensure that you can contact the DNS servers from both the servers. You must do this before you configure HA Failover. If DNS is configured but DNS servers are not accessible, SSH communication can be delayed. The delay can cause the HA Failover configuration to fail.
7. Ensure that you can contact either NTP server from both the servers or that you can disable NTP on both the servers. You must do this before you configure HA Failover. If NTP is configured but the NTP servers are not accessible, SSH communication can be delayed. The delay can cause the HA Failover configuration to fail.
8. If the System Platform HA Failover is configured, you can start the HA Failover from the preferred node Web console Failover Web page. The system redirects the Web console to restart the Web page for about 5 minutes. Then the system redirects you to the log-in page, and you can log in again.

Must read while performing System Platform-based HA

- Install the template on the standby node.
- You cannot install the template on a system with a running HA Failover.
- You cannot make network configuration changes on a system with a running HA Failover.

Appendix G: Resetting the admin user password

To reset the System Manager Web Console admin user password:

- Log in to the System Manager command line interface (CLI) as a **root** user. If direct CLI access is not enabled for the **root user** then log in as admin with direct access to CLI and then escalate access privileges restrictions by issuing the **su** command at the server CLI.

1. Run the following command to create a **securityadmin** group:
   groupadd -g 600 securityadmin

   - If the system displays the error message groupadd: GID 600 is not unique, then use a higher value instead of 600 and run the same command.
   - If the system displays the error message groupadd: group securityadmin exists, then the group is already present and you do not have to create the group again.

2. Run the groups **admin** command to verify whether the user **admin** has the securityadmin group assigned to the user. This might happen if the group securityadmin was already present and assigned to user admin.
   The output of the command must not mention **securityadmin** in the list of groups assigned to user **admin**.

3. If the output of Step 3 mentions that group **securityadmin** is not assigned to user **admin**,run the following command to assign the group to the user:

   usermod -aG securityadmin admin

4. Gain access to the System Manager local log-in screen at https://<IP Address/Fully Qualified Hostname>/local-login.

5. Use the log-in credentials of the System Manager CLI user **admin** to log in. After the system displays the **Security Configuration** screen, change the URL to:
   https ://< System Manager IP Address/Fully Qualified Hostname>/passwordReset

6. After the system displays the **Password Reset** screen, specify the user ID as admin and the new password as **admin123**.

7. After the system displays the message Password changed successfully, close the current browser session and gain access to the System Manager log-in screen in a new browser session at:

   https ://< System Manager IP Address/Fully Qualified Hostname>/SYSTEM MANAGER

   If you gain access to System Manager using

   - A fully qualified host name:

a. Log in using the password specified in Step 7, **admin123**.
b. At the system prompt, specify the new password.

- An IP address:
  a. Click the **Change Password** link on the log-in page, and change the password.
  b. Open the System Manager log-in screen again, and log in using the new password.

8. If the group securityadmin was assigned to user **admin** in Step 4, then perform the following steps to unassign the group **securityadmin** from user **admin**:
   a. Run the following command on System Manager CLI as a root user to list the groups assigned to user admin:

   ```
   groups admin
   ```

   Assume the output is:

   ```
   admin: admin xxx securityadmin xyz
   ```

   Run the following command to unassign the group **securityadmin** from user **admin:**

   ```
   usermod -G <list of comma separated groups except securityadmin> admin
   ```

   As per the example, the command should be:

   ```
   usermod -G admin,abc,xyz admin
   ```

9. If you created the group **securityadmin** in Step 2, then run the following command to delete the group:

   ```
   groupdel securityadmin
   ```

Appendix H: Profile Change for Serviceability Agent

If the there is change in SDOM's IP-Address where SAL GW was previously deployed, then that SAL Gateway's profile at the System Manager has to be changed.

The Profile can be changed from System Manager Web Console for System Manager-Serviceability Agent as follows:

1. From System Manager Dashboard select **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.
2. From the Serviceability Agents page, select the serviceability agent of System Manager and click **Manage Profiles**.
3. From the Manage Profiles page, select the **SNMP Target profiles** tab and remove the SAL Gateway's profile and click **Commit**.
4. Select **Manage Serviceability Agents** > **SNMP Target Profiles**.
5. From SNMP Target Profiles page, select the SAL Gateway profile and edit the IP-Address information of the profile.
6. Select **Manage Serviceability Agents** > **Serviceability Agents**.
7. From the Serviceability Agents page, select the serviceability agent of System Manager and click **Manage Profiles**.
8. From the Manage Profiles page, select the **SNMP Target profiles** tab and assign the edited SAL Gateway profile and click **Commit**.

The Profile can be changed from System Manager UI for Adopter's-Serviceability Agent as follows:

1. From System Manager Dashboard select **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.
2. From the Serviceability Agents page select all the serviceability agents which have the SAL Gateway profile attached and click Manage Profiles.
3. From the Manage Profiles page, select the **SNMP Target profiles** tab and remove the SAL Gateway's profile and click **Commit**.
4. Select **Manage Serviceability Agents** > **SNMP Target Profiles**.
5. From SNMP Target Profiles page select the SAL Gateway profile and edit the IP-Address information.
6. Select **Manage Serviceability Agents** > **Serviceability Agents**.
7. From the Serviceability Agents page then select all the serviceability agents where you want to assign the edited SAL Gateway profile and click **Manage Profiles**.
8. From the Manage Profiles page, select the SNMP Target profiles tab and assign the edited SAL Gateway profile and click **Commit**.