Migrating the Avaya Aura® System Manager data to 6.3 using Data Migration Utility

Release 6.3
Issue 1
May 2013

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees 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 End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). 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 to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. 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 you. “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.

License type

Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

Each vAppliance will have its own ordering code. Note that each instance of a vAppliance must be separately ordered. If the end user customer or Business Partner would like to install two of the same type of vAppliances, then two vAppliances of that type must be ordered.

Each Product has its own ordering code. Note that each instance of a Product must be separately licensed and ordered. “Instance” means one unique copy of the Software. For example, if the end user customer or Business Partner would like to install two instances of the same type of Products, then two Products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright

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 Toll 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 website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

This document provides procedures for upgrading Avaya Aura® System Manager from earlier releases to Release 6.3.2 on System Platform. The document includes upgrade checklist and procedures for upgrade and verification.

Intended audience

The primary audience for this document is anyone who is involved with upgrading, maintaining, and verifying System Manager on at a customer site. The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers.

Document changes since last issue

The following changes have been made to this document since the last issue:

- Added procedures for migrating System Manager to Release 6.3.2 using the data migration utility.
- Added procedures for installing the System Manager 6.3.2 patch.

Related resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com

Document number	Title	Description	Audience
Design			
	Understanding Avaya Aura® System Manager	Describes the key features of System Manager and the shared management services that System Manager provides for Avaya Aura® applications.	Sales Engineers, Solution Architects, Implementation Engineers, and Support personnel
	Avaya Aura® System Manager Overview and Specification	Describes tested product characteristics and capabilities including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.	Sales Engineers, Solution Architects, Implementation Engineers, and Support personnel
Implementation			
	Implementing Avaya Aura® System Manager	Describes the procedures to install, configure System Manager and the managed elements that System Manager supports.	Implementation Engineers and Support personnel
-	Avaya Aura® System Manager using VMware® in the Virtualized Environment Deployment Guide.	Describes the procedures for deploying the Avaya Aura® System Manager virtual application in the Avaya Aura® Virtualized Environment.	Implementation Engineers and Support personnel

Document number	Title	Description	Audience
03-603793	Installing the Dell™ PowerEdge™ R610 server	Describes the procedures to install the Dell™ PowerEdge™ R610 server.	Implementation Engineers and Support personnel
03-603799	Installing the HP ProLiant DL360 G7 server	Describes the procedures to install the HP ProLiant DL360 G7 server.	Implementation Engineers and Support personnel
	Installing and Configuring Avaya Aura® System Manager	Describes the procedures to install and troubleshoot System Platform.	Implementation Engineers and Support personnel
Maintenance and Troubleshooting			
	Troubleshooting Avaya Aura® System Manager	Describes the procedures to troubleshoot the problems during the installation and administration of System Manager and the managed elements that System Manager supports.	Implementation Engineers and Support personnel
Administration			
	Administering Avaya Aura® System Manager	Describes the procedures to configure System Manager and the managed elements that System Manager supports.	Implementation Engineers and Support personnel

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After logging into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Course code	Course title	Type
5U00106W	Avaya Aura® System Manager Overview	Web/On Demand
5U00095V	Avaya Aura® System Manager Implementation, Administration, Maintenance and Troubleshooting	virtual Instructor-Led Training (vILT)

Course code	Course title	Type
5U00103 W	Avaya Aura® System Manager 6.2 Delta Overview	Web/On Demand

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Go to http://www.youtube.com/AvayaMentor and perform one of the following actions:

- Enter a key word or key words in the Search Channel to search for a specific product or topic.
- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Warranty

Avaya provides a 90-day limited warranty on the System Manager software. For detailed terms and conditions, see the sales agreement or other applicable documentation. Additionally, for the standard warranty description of Avaya and the details of support, see **Help & Policies** > **Policies & Legal** > **Maintenance and Warranty Information** on the Avaya Support website at http://support.avaya.com. For additional information, see **Help & Policies** > **Policies & Legal** > **License Terms**.

For more details on the hardware maintenance for supported products, see http://portal.avaya.com/ptlWeb/services/SV0452.

Data migration overview

This document provides the procedures for migrating the Avaya Aura® System Manager data from earlier releases to System Manager Release 6.3.2 running on System Platform.

Depending on the System Manager release, you can use one of the following methods to migrate the System Manager data:

- Data migration from System Manager 5.2.x to Release 6.3.2 using the Network Routing Policy (NRP) export and import utility. To migrate the System Manager data from Release 5.2.x, on the 5.2.x system, export the data using by the NRP export utility and then import the data using the NRP import utility to the Release 6.3 system.
- Data migration from Release 6.x to Release 6.3.2 using the data migration utility. To migrate the System Manager data from Release 6.x, use the data migration utility from the command line interface (CLI).

> ❗ **Important:**
>
> You can run the data migration utility only on System Manager Release 6.3. You cannot run the data migration utility on System Manager Release 6.3 on which you installed a service pack. If a service pack is already running on System Manager Release Release 6.3, delete the template, install the System Manager Release 6.3 template, and run the data migration utility.

Release 6.3.x supports the following servers:

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

You can also upgrade the earlier releases of System Manager running on System Platform to Release 6.3.2 by using the procedures described in *Upgrading Avaya Aura® System Manager to Release 6.3.2*.

For procedures to upgrade the Avaya Aura® System Manager virtual application in the Avaya Aura® Virtualized Environment, see *Avaya Aura® System Manager using VMware® in the Virtualized Environment Deployment Guide*.

Data Migration utility

Use the Data Migration utility to migrate the backup data of System Manager 6.x directly to System Manager Release 6.3. In the data migration process, you do not have to perform the intermediate steps involved in upgrading System Manager and System Platform as outlined in *Administering Avaya Aura® System Manager* .

Using the data migration process, you can perform faster software-only upgrades or software and hardware upgrades without any delays during the upgrade process.

NRP import and export utility

Using the NRP utility, you can perform data migration by importing and exporting the data related to NRP. You cannot migrate the data related to other System Manager options. Use the NRP utility only to import and export the System Manager 5.2 data to System Manager 6.3.

Chapter 2: Data migration from System Manager 5.2

Overview

During the migration of the data from System Manager Release 5.2 to Release 6.3.2, the system only retains the Network Routing Policy (NRP) data. You must manually add the remaining System Manager data to the Release 6.3.2 system.

Checklist for data migration from System Manager 5.2

The data migration from System Manager 5.2 to Release 6.3 procedure involves the following high-level tasks. Perform the tasks sequentially.

#	Field	Notes	✔
1	Verify the software version of the current System Manager.		
2	Create a backup of the System Manager data.		
3	Export the data from System Manager Release 5.2.x.		
4	Record the System Platform configuration data such as SAL Gateway configuration, static routes, High Availability (HA) configuration data, and users.	You require the data to reconfigure the new System Platform installation.	

#	Field	Notes	✔
5	If the existing server is not compatible with System Manager 6.3.x, change the server.	Release 6.2 and later supports the following servers: • IBM x3550m2 • HP ProLiant DL360 G7 2CPU MID4 • Dell™ PowerEdge™ R610 2CPU MID2	
6	On the supported server, install the System Platform Release 6.3.0.0.18002 software.	• For instructions to install a new server, see *Installing the HP ProLiant DL360 G7 Server*, 03-603799 or *Installing the Dell™ PowerEdge™ R610 Server*, 03-603793. • For instructions to install System Platform, see Installation methods on page 41. ✱ **Note:** If the existing system has High Availability (HA) configured on it, stop HA. Also, you can start the System Platform installation on the standby server. For instructions to stop HA, see Stopping System Platform High Availability on page 99.	
7	Install the System Manager Release 6.3 template.	Installing the System Manager template using ISO on page 102.	
8	Install the `System_Manager_R6.3_FP2_S4_1399.bin` file.		
9	Copy the backup file on System Manager Release 6.3.2.		
10	Import the data to System Manager Release 6.3.2.	Importing the data to 6.3 on page 18.	
11	Verify that the functionality of the current System Manager works properly.		
12	Reconfigure System Platform with the data that you recorded in Step 4. You can also start HA. For instructions, see		

#	Field	Notes	✔
	Starting System Platform High Availability on page 99.		
13	Create a backup of the System Manager data.		

Verifying the current software version

Use this procedure to verify the current software version for System Manager 1.0 or 5.2.

System Manager 1.0 or 5.2 does not display the **About** link on the dashboard. Therefore, to determine the version ID use the `inventory.xml` file.

Before you begin

Ensure that you apply the correct software patch on System Manager.

Procedure

1. From the command line interface (CLI), log in to the System Manager.
2. At the prompt, enter `# vi /opt/Avaya/installdata/inventory.xml`.
3. In the `inventory.xml` file, search for the term System Manager and note the version ID.
4. Verify the version number of System Manager with the highest build number for the release.

Related topics:

Compatibility matrix for the System Manager and System Platform software versions on page 125

System Manager and System Platform patches on page 127

Creating a data backup on a remote server

Before you begin

Log on to System Manager Web Console as `admin`.

Procedure

1. Click **Settings** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. To back up the data to a remote location, on the Backup page:
   a. Click **Remote**.
   b. Enter the details in the **SCP server IP**, **SCP server port**, **User name**, **Password**, and the file name in the respective fields.
4. Click **Now**.
   If the backup is successful, the Backup and Restore page displays `Backup created successfully!!`

Exporting the data from System Manager 5.2

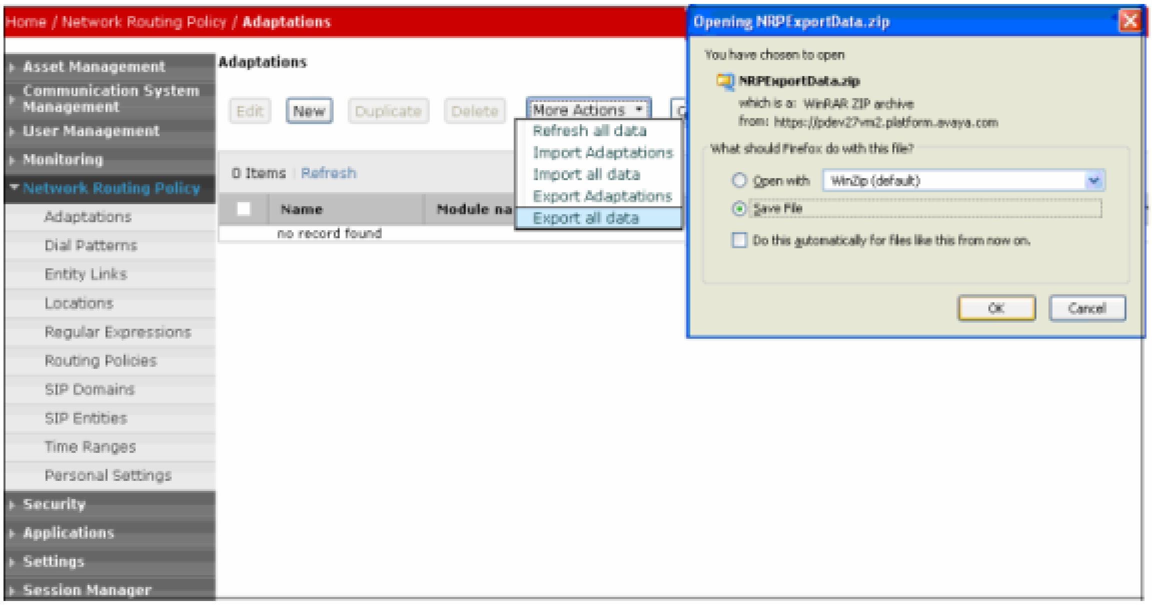
Perform this procedure to migrate the System Manager data from Release 5.2 and 5.2 SP 1 to System Manager Release 6.3.

Before you begin

- Create a backup of the System Manager 5.2 data.
- Record the NRP records on System Manager 5.2. To view the records, on the Web Console of System Manager 5.2, click **Routing** > **Policies**. After you import the data, you require these records to verify if the system has successfully imported the data on System Manager Release 6.3.
- Record the data related to users, custom roles, and configuration. After importing the NRP data, you must manually add the data to System Manager Release 6.3.
- Record the network parameters on System Manager 5.2.

Procedure

1. To log on to System Manager Web Console, in a Web browser, enter `https://<IPAddress of System Manager>/SMGR`.
2. Log on to System Manager Web Console using the administrator credentials made available at the time of the System Manager installation.
3. Click **Network Routing Policy** > **Adaptations**.
4. On the Adaptations page, click **More Actions** > **Export All Data**.



Opening NRPExportData.zip

You have chosen to open

NRPExportData.zip

which is a: WinRAR ZIP archive

from: https://pdev27vm2.platform.avaya.com

What should Firefox do with this file?

○ Open with WinZip (default)

● Save File

□ Do this automatically for files like this from now on.

5. Save the `NRPExportData.zip` file to a location that you can easily access.
6. Shut down the server on which System Manager is running.

Installing System Platform

Before you begin

Log on to System Platform Web Console.

Procedure

1. Obtain the System Platform Release 6.3.0.0.18002 software from the PLDS website at https://plds.avaya.com.
2. On the server, install System Platform Release 6.3.0.0.18002. For instructions, see Installation methods.

   The network configuration for System Platform must be the same as the network configuration of System Manager.

Installing the System Manager template

Before you begin

Download the software for the System Manager 6.3 template.

Procedure

1. Log on to System Platform Web Console using the administrator credentials made available at the time of the System Platform installation.
2. Install the System Manager template. For instructions, see Installing the SMGR template using ISO on page 102.

Next steps

To gain access to System Manager Web Console, perform one of the following actions:

- In the Web browser, enter `https://<Fully qualified domain name of System Manager>`.
- On the System Platform Web Console, perform the following:
    a. Click **Home**.
    b. In the **Virtual Machine List** section, click the wrench icon (🔧) adjacent to the SMGR link.

       The system opens the System Manager login page.

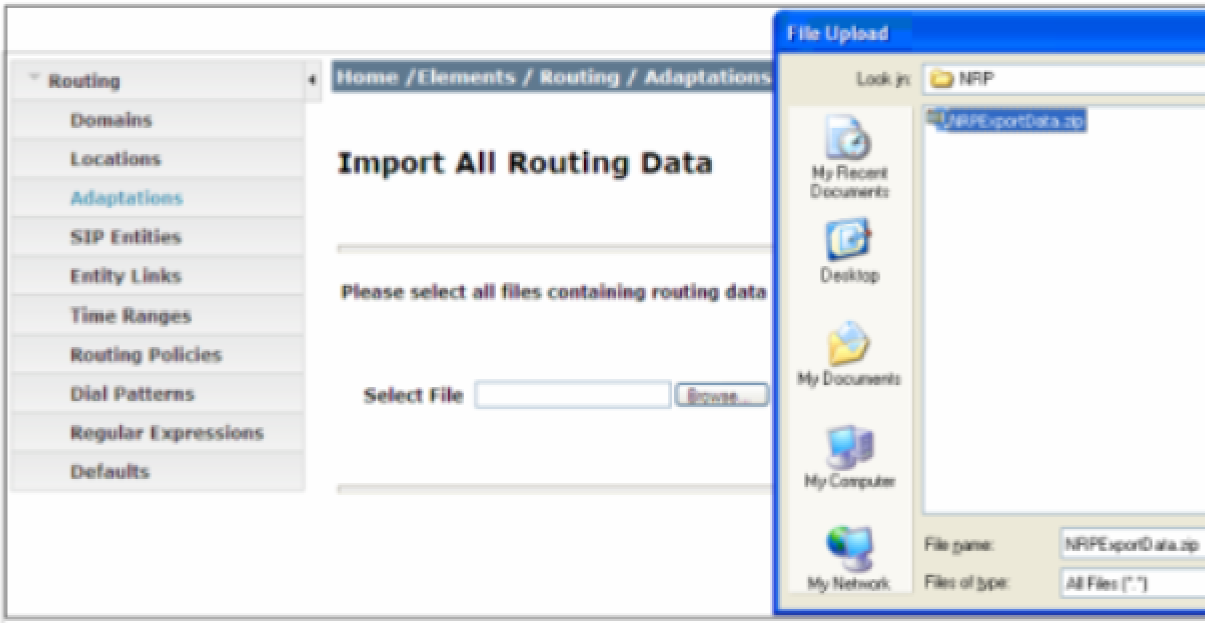
Importing the data to System Manager Release 6.3

Perform this procedure on System Manager 5.2.x to migrate the System Manager data from Release 5.2, 5.2 SP1, and 5.2 SP2 to System Manager Release 6.3.

Procedure

1. To log in to the System Manager Web Console, in the Web browser, enter `https://<fully qualified domain name of System Manager>/SMGR`.
2. Log in to System Manager Web Console using the administrator credentials made available at the time of the System Manager installation.
3. Click **Elements** > **Routing** > **Adaptations**.

4. On the Adaptations page, click **More Actions** > **Import**.
5. To upload the file, on the Import All Routing Data page, browse to the `NRPExportData.zip` file.



6. To import the NRP data, click **Import**.
7. Verify that the NRP data is successfully imported to System Manager Release 6.3.
8. Create users, custom roles, and configuration that you recorded on System Manager 5.2.x.

Installing the System Manager 6.3.2 patch

Procedure

1. Obtain the System Manager 6.3.2 patch `System_Manager_R6.3_FP2_S4_1399.bin` from the PLDS website at https://plds.avaya.com. For instructions to download the patch, see Downloading patches.
2. Log on to System Platform Web Console and install the `System_Manager_R6.3_FP2_S4_1399.bin` file. For instructions, see Installing patches.

3. Verify that the patch installation is successful and click **Commit**.

Related topics:

Downloading patches on page 111

Installing patches on page 112

Creating a data backup on a remote server

Procedure

1. On System Manager Web Console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Remote**.
4. Perform one of the following:
   - Perform the following:
     i. In the **File transfer protocol** field, click `SCP` or `SFTP`.

     ii. Specify the remote server IP, remote server port, user name, password, and name and the path of the backup file that you create.
   - Select the **Use Default** check box.

   Important:

   To use the **Use Default** option, ensure that you specify the remote server IP, user name, password, and name and path of the backup file on the SMGR Element Manager Container page. To open the SMGR Element Manager Container page, click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.
5. Click **Now**.
   If the backup is successful, the Backup and Restore page displays the message:
   ```
   Backup job submitted successfully. Please check the status
   detail below!!
   ```

Related topics:

Recommendations for System Manager data backup on page 119

Chapter 3: Data migration from System Manager 6.x

Overview

Use this section to migrate the data from the following System Manager releases to System Manager Release 6.3.2:

- 6.0 SP1 or SP2
- 6.1 SP1.1, SP2, SP3, SP4, SP5, SP6, SP7, or SP8
- 6.2 SP1, SP2, SP3, or SP4

Prerequisites

#	Prerequisite	Notes
1	Obtain the following software from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com. • System Platform 6.2.1.0.9 and the System Platform 6.2.2.06002.0 patch. • The System Manager Release 6.3 template • The Data Migration utility, `dmutility-6.3-DataMigration-*.bin`	

#	Prerequisite	Notes
2	Verify that the existing server is compatible with System Manager 6.3.x. If the existing server is not compatible, you must change the server as instructed in the workflow described in this chapter.	Release 6.3.x supports the following servers: • IBM x3550m2 • HP ProLiant DL360 G7 2CPU MID4 • Dell™ PowerEdge™ R610 2CPU MID2
3	Keep the following checklists handy: • The System Manager Release 6.3 installation checklist • The data migration checklist	
4	Keep the following information handy to create a backup on the remote server: • IP address • Directory • User Name • Password	
5	Record the number of users and custom roles in the current release of System Manager. After the migration, you require this data to verify if the system has successfully imported the users and roles from the earlier release to System Manager Release 6.3.	For more information, see “Managing users” and “Managing roles” sections in *Administering Avaya Aura® System Manager*.

Related topics:

Checklist for data migration from System Manager 6.x on page 24
System Manager installation checklist on page 121

Upgrade paths that support the data migration utility

To System Manager	Release 6.3 on System Platform	Release 6.3.0 on VMware	Release 6.3.2 on VMware
From System Manager			
Release 6.0 on System Platform	✔	✔	✔
Release 6.1 on System Platform	✔	✔	✔
Release 6.2 on System Platform	✔	✔	✔
Release 6.2 on VMware	X	✔	✔
Release 6.3 on System Platform	X	X	X
Release 6.3.2 on System Platform	X	X	X
Release 6.3.2 on VMware	X	X	X

✔	Supported
X	Not applicable

Data migration worksheet

For the System Manager installation checklist and worksheet, see System Manager installation checklist on page 121 and System Manager information worksheet on page 123.

#	Field	Value	Notes
1	**IP address of external device for remote backup**		On the remote backup page of the System Manager Web Console, enter the IP address of

#	Field	Value	Notes
			the remote machine on which the backup file is located.
2	**User Name and Password of the remote server**		To gain access to the backup file that is located on a remote server, enter the user name and the password of the account on the System Manager Web Console.
3	**System Manager CLI credential**		Open an SSH session and enter `admin` as the user name and password.
4	**Root password of SMGR machine**		On the CLI, to change to root, type the **`su -`** command.
5	**Path and the file name of the backup file on the remote server**		Enter the path and the file name of the backup file.

Checklist for data migration from System Manager 6.x

The data migration from System Manager Release 6.0.x, 6.1.x, or 6.2.x to Release 6.3.2 involves the following tasks. Perform the tasks sequentially.

#	Task	Notes	✔
1	Verify that the RAID Controller battery level is not low. If the battery level is low, replace the battery before you proceed with the upgrade.	If the RAID Controller battery depletes, the Disk Cache policy is set to WriteThrough. As a result, the overall system operations slow down and the duration of the upgrade process increases. For additional information, see the S8800 or HP ProLiant DL360 G7 server RAID on the Avaya Support website at http://support.avaya.com/.	

#	Task	Notes	✔
2	Verify the software version of the current System Manager.		
3	Create a backup of the System Manager data.		
4	Record the System Platform configuration data such as SAL Gateway configuration, static routes, High Availability (HA) configuration data, and users.	You require the data to reconfigure the new System Platform installation.	
5	If the existing server is not compatible with System Manager 6.3.x, change the server.	Release 6.2 and later supports the following servers: • IBM x3550m2 • HP ProLiant DL360 G7 2CPU MID4 • Dell™ PowerEdge™ R610 2CPU MID2	
6	On the supported server, install the System Platform Release 6.3.0.0.18002 software.	• For instructions to install a new server, see *Installing the HP ProLiant DL360 G7 Server*, 03-603799 or *Installing the Dell™ PowerEdge™ R610 Server*, 03-603793. • For instructions to install System Platform, see Installation methods on page 41. **Note:** If the existing system has High Availability (HA) configured on it, stop HA. Also, you can start the System Platform installation on the standby server. For instructions to stop HA, see Stopping System Platform High Availability on page 99.	
7	Install the System Manager Release 6.3 template.	Installing the System Manager 6.3 template using ISO on page 102.	
8	Install the `System_Manager_R6.3_FP2_S4_1399.bin` file.		

#	Task	Notes	✔
9	Copy the backup file on System Manager Release 6.3.2.		
10	On System Manager 6.3, run the dmutility-6.3-DataMigration-20130213.085948-86.bin file from the command line interface (CLI).		
11	Verify that the functionality of the current System Manager works properly.		
12	Reconfigure System Platform with the data that you recorded in Step 4. You can also start HA. For instructions, see Starting System Platform High Availability on page 99.		
13	Create a backup of the System Manager data.		

Checklist for data migration from System Manager configured with Geographic Redundancy

The data migration from System Manager 6.x configured with Geographic Redundancy to Release 6.3 procedure involves the following tasks. Perform the tasks sequentially.

#	Field	Notes	✔
1	Verify the software version of the current System Manager.		
2	Create a backup of the System Manager data.		
3	Disable the Geographic Redundancy replication.	See *Administering Avaya Aura® System Manager*.	
4	Run the `dmutility-6.3-DataMigration-*.bin` file from the command line interface (CLI).		
5	Verify that the functionality of the current System Manager works properly.		

#	Field	Notes	✔
6	On the primary System Manager server, enable the Geographic Redundancy replication.	See *Administering Avaya Aura® System Manager*.	

Verifying the current software version

Before you begin

Ensure that you apply the correct software patch on System Manager.

About this task

Use this procedure to verify the current software version for System Manager 6.x.

Procedure

1. Log on to System Manager Web Console.
2. To view the build number, in the top-right corner of the Web console, click **About**.

   The system displays the About SMGR window with the build details.
3. Verify the version number of System Manager with the highest build number for the release.

Related topics:

Compatibility matrix for the System Manager and System Platform software versions on page 125

System Manager and System Platform patches on page 127

Creating a data backup on a remote server

Procedure

1. Perform one of the following:
   - For System Manager 6.1 and later, on System Manager Web Console, click **Services** > **Backup and Restore**.
   - For System Manager 6.0, on System Manager Web Console, click **System Manager Data** > **Backup and Restore**.

2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Remote**.
4. Specify the remote server IP, remote server port, user name, password, and name and path of the backup file that you create.
5. Click **Now**.
   If the backup is successful, the Backup and Restore page displays the message: `Backup job submitted successfully. Please check the status detail below!!`

Related topics:
Recommendations for System Manager data backup on page 119

Installing System Platform

Before you begin

Log on to System Platform Web Console.

Procedure

1. Obtain the System Platform Release 6.3.0.0.18002 software from the PLDS website at https://plds.avaya.com.
2. On the server, install System Platform Release 6.3.0.0.18002. For instructions, see Installation methods.

   The network configuration for System Platform must be the same as the network configuration of System Manager.

Installing the System Platform patch

Procedure

1. Obtain the 6.2.2.06002.0 patch for System Platform from the PLDS website at https://plds.avaya.com. For instructions to download the patch, see Downloading patches.
2. Install the 6.2.2.06002.0 patch on System Platform Release 6.2.1.0.9. For instructions, see Installing patches.

Installing the System Manager template

Before you begin

Download the software for the System Manager 6.3 template.

Procedure

1. Log on to System Platform Web Console using the administrator credentials made available at the time of the System Platform installation.
2. Install the System Manager template. For instructions, see Installing the SMGR template using ISO on page 102.

Next steps

To gain access to System Manager Web Console, perform one of the following actions:

- In the Web browser, enter `https://<Fully qualified domain name of System Manager>`.
- On the System Platform Web Console, perform the following:
    a. Click **Home**.

    b. In the **Virtual Machine List** section, click the wrench icon (🔧) adjacent to the SMGR link.

    The system opens the System Manager login page.

Upgrading to System Manager 6.3.x using the data migration utility

Before you begin

- Download the data migration utility, `dmutility-6.3-DataMigration-*.bin` file, from the PLDS website at http://plds.avaya.com.
- Start an SSH session.

Procedure

1. Log on to System Manager Web Console.
2. Copy the following files to the `/home/admin` location on the System Manager Release 6.3.

- The System Manager backup (`.zip`) file
- The `dmutility-6.3-DataMigration-*.bin` file

3. Record the system parameters and network parameters of System Manager.
4. Shut down the System Manager machine.
5. Install the System Manager template.

   Important:

   Use the same network parameters and system parameters that you recorded in Step 3.
6. Log in to the command line interface of System Manager and obtain the access to root.
7. To assign the permission to run the data migration utility file, at the prompt of the SSH console, type `chmod +x dmutility-6.3-DataMigration-*.bin`.
8. Type `# ./dmutility-6.3-DataMigration-*.bin -m -v`.
9. Type the complete path to the backup file.
10. At the prompt, confirm to proceed with the upgrade.

    The system upgrades the System Manager data in the verbose mode. The upgrade process might take some time to complete. Wait until the upgrade process is complete before you continue with the next step. During this time, you cannot gain access to System Manager Web Console.

Verifying the functionality of System Manager

To ensure that System Manager is working correctly after the data migration is complete, verify that the current installation of System Manager is successful.

About this task

Note:

When you migrate to System Manager Release 6.3 from release:

- 6.0.x or 6.1.x. If you have users with roles other than *admin*, the system resets the user passwords to the login name of the users.

  For example, the system sets the password of a user with the login name dsmith@avaya.com and a role other than End-User to dsmith@avaya.com after the migration.

The end user passwords in System Manager Release 6.3 or 6.2 remain the same as in 6.1.

- 6.0.x. The system resets the admin password.
- 6.1.x or 6.2.x. The admin password remains the same.

When you promote an end user to an administrator, the system resets the password for the end user to the login name of the user.

Procedure

1. To log on to the System Manager Web Console, in the Web browser, enter `https://<FQDN>/SMGR`, where *FQDN* is the fully qualified domain name of System Manager.
2. On the upgraded system, verify that the following data matches the number of users and roles that you recorded before the upgrade.
    - The number of users
    - The number of roles

   For more information, see “Managing users” and “Managing roles” sections in *Administering Avaya Aura® System Manager*.
3. Verify if the following function correctly:
    - Creation and deletion of a user
    - Creation of a role
    - Creation of a job
    - Creation of the remote data backup
    - Replication of the data using Data Replication Service (DRS)

   For instructions to complete each verification task, see *Administering Avaya Aura® System Manager*.

Installing the System Manager 6.3.2 patch

Procedure

1. Obtain the System Manager 6.3.2 patch `System_Manager_R6.3_FP2_S4_1399.bin` from the PLDS website at https://plds.avaya.com. For instructions to download the patch, see Downloading patches.

2. Log on to System Platform Web Console and install the `System_Manager_R6.3_FP2_S4_1399.bin` file. For instructions, see Installing patches.
3. Verify that the patch installation is successful and click **Commit**.

Related topics:

Downloading patches on page 111

Installing patches on page 112

Creating a data backup on a remote server

Procedure

1. On System Manager Web Console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Remote**.
4. Perform one of the following:
   - Perform the following:
     i. In the **File transfer protocol** field, click `SCP` or `SFTP`.
     ii. Specify the remote server IP, remote server port, user name, password, and name and the path of the backup file that you create.
   - Select the **Use Default** check box.

   Important:

   To use the **Use Default** option, ensure that you specify the remote server IP, user name, password, and name and path of the backup file on the SMGR Element Manager Container page. To open the SMGR Element Manager Container page, click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.
5. Click **Now**.
   If the backup is successful, the Backup and Restore page displays the message: `Backup job submitted successfully. Please check the status detail below!!`

Related topics:

Recommendations for System Manager data backup on page 119

Appendix A: Common procedures for System Manager data migration

Overview

This section provides common procedures that you must perform during the System Manager data migration process.

Note:

Perform the procedures listed in this section only when instructed.

Installing System Platform

Preinstallation tasks for System Platform

Preinstallation checklist for System Platform

Before starting System Platform installation, make sure that you complete the tasks from the following preinstallation checklist.

No.	Task	Notes	✔
1	Complete and submit the Universal Install/SAL Product Registration Request form. When opening the Excel based form, click **Enable Macros**; otherwise, the form automation will not work. Submit the completed form using the built in e-mail	**Important:** Submit the registration form three weeks before the planned installation date.	

No.	Task	Notes	✔
	button. See Registering the system on page 36.		
2	Gather the required information relating to installation, such as IP configuration information, DNS addresses, and address information for Network Time Protocol (NTP) servers. See Installation worksheet for System Platform.		
3	Register for PLDS unless you have already registered. See Registering for PLDS on page 38.		
4	Download the System Platform installer ISO image file from PLDS. See Downloading software from PLDS on page 38.		
5	Download the appropriate solution template and licenses from PLDS. See Downloading software from PLDS on page 38.		
6	Verify that the downloaded ISO images match the images on the PLDS Web site. See Verifying the ISO image on a Linux-based computer on page 39 and Verifying the ISO image on a Windows-based computer on page 39.		
7	Write the ISO images to separate DVDs. See Writing the ISO image to DVD or CD on page 40.	**Note:** If the software files you are writing on media are less than 680 Mb in size, you can use a CD instead of a DVD.	

Registering the system

About this task

Registering System Platform and applications in the solution template ensures that Avaya has a record of the system and it is ready for remote support if needed.

Avaya assigns a Solution Element ID (SE ID) and Product ID to each SAL Gateway and managed device that is registered. In the context of System Platform, managed devices are the components of System Platform and of the applications that are included in the solution template. The SE ID makes it possible for Avaya Services or Avaya Partners to connect to the managed applications remotely. The Product ID is included in alarms that are sent to alarm receivers from the managed device. The Product ID identifies the device that generated the alarm. This data is critical for correct execution of various Avaya business functions and tools.

Note:

- For a description of any elements you must register along with your Solution Template, see your Avaya Aura® solution documentation.
- For solutions being deployed in a System Platform High Availability configuration, you must register two VSP solution elements, one for the primary server and one for the secondary server in the HA pair. For a description of any other solution elements you must register for the various System Platform High Availability deployments, see your Avaya Aura® solution documentation.

Registrations are performed in two stages: before installation of System Platform, the solution template, and SAL Gateway and after installation. The first stage of registration provides you with the SE IDs and Product Identifications required to install the products. The second stage of the registration makes alarming and remote access possible.

Procedure

1. Access the registration form and follow the instructions. This form is available at http://support.avaya.com. In the navigation pane, click **More Resources** > **Avaya Equipment Registration**. Under Non-Regional (Product) Specific Documentation, click **Universal Install/SAL Product Registration Request Form**, or search *Universal Install/SAL Product Registration Request Form*.
2. Complete the Universal Install Product Registration page and submit it at least three weeks before the planned installation date.

   Provide the following:

   - Customer name
   - Avaya Sold-to Number (customer number) where the products will be installed
   - Contact information for the person to whom the registration information should be sent and whom Avaya can contact if any questions arise
   - Products that are included in the solution template and supporting information as prompted by the form

   Avaya uses this information to register your system. When processing of the registration request is complete, Avaya sends you an e-mail with an ART install script attached. This script includes instructions for installation and the SE IDs and Product IDs that you must enter in SAL Gateway to add managed devices.
3. Complete and submit the Universal Install Alarm Registration page after the installation is complete.

Related topics:

[SAL Gateway](#) on page 68
[Configuration prerequisites](#) on page 70
[Gateway Configuration field descriptions](#) on page 73

Registering for PLDS

Procedure

1. Go to the Avaya Product Licensing and Delivery System (PLDS) Web site at https://plds.avaya.com.
   The PLDS Web site redirects you to the Avaya single sign-on (SSO) Web page.
2. Log in to SSO with your SSO ID and password.
   The PLDS registration page is displayed.
3. If you are registering:
   - as an Avaya Partner, enter the Partner Link ID. If you do not know your Partner Link ID, send an e-mail to prmadmin@avaya.com.
   - as a customer, enter one of the following:
     - Company Sold-To
     - Ship-To number
     - License authorization code (LAC)
4. Click **Submit**.
   Avaya will send you the PLDS access confirmation within one business day.

Downloading software from PLDS

About this task

✱ **Note:**

You can download product software from http://support.avaya.com also.

Procedure

1. Type `http://plds.avaya.com` in your Web browser to go to the Avaya PLDS website.
2. Enter your Login ID and password to log on to the PLDS Web site.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.

5. Search for the available downloads using one of the following methods:
    - By actual download name
    - By selecting an application type from the drop-down list
    - By download type
    - By clicking **Search Downloads**
6. Click the download icon from the appropriate download.
7. When the system displays the confirmation box, select **Click to download your file now**.
8. If you receive an error message, click on the message, install Active X, and continue with the download.
9. When the system displays the security warning, click **Install**.

    When the installation is complete, PLDS displays the downloads again with a checkmark next to the downloads that are completed successfully.

Verifying the downloaded ISO image

Verifying the ISO image on a Linux-based computer

About this task

Use this procedure to verify that the md5 checksum of the downloaded ISO image matches the md5 checksum that is displayed for the ISO image on the PLDS Web site.

Use this procedure if you downloaded ISO images to a Linux-based computer.

Procedure

1. Enter `md5sum` *`filename`*, where *filename* is the name of the ISO image. Include the .iso file extension in the filename.
2. Compare the md5 checksum of the ISO image to be used for installation with the md5 checksum that is displayed for the ISO image on the PLDS Web site.
3. Ensure that both numbers are the same.
4. If the numbers are different, download the ISO image again and reverify the md5 checksum.

Verifying the ISO image on a Windows-based computer

About this task

Use this procedure to verify that the md5 checksum of the downloaded ISO image matches the md5 checksum that is displayed for the ISO image on the PLDS Web site.

Use this procedure if you downloaded ISO images to a Windows-computer.

Procedure

1. Download a tool to compute md5 checksums from one of the following Web sites:
    - http://www.md5summer.org/
    - http://code.kliu.org/hashcheck/

    Note:

    Avaya has no control over the content published on these external sites. Use the content only as reference.
2. Run the tool on the downloaded ISO image and note the md5 checksum.
3. Compare the md5 checksum of the ISO image to be used for installation with the md5 checksum that is displayed for the ISO image on the PLDS Web site.
4. Ensure that both numbers are the same.
5. If the numbers are different, download the ISO image again and reverify the md5 checksum.

Writing the downloaded software to DVD

DVD requirements

Use high quality, write-once, blank DVDs. Multiple rewrite DVDs are prone to error and should not be used.

When writing the data to the DVD, use a slower write speed of 4X or a maximum 8X. Attempting to write to the DVD at higher or the maximum speed rated on the disc is likely to result in write errors.

Note:

If the software files you are writing on media are less than 680 Mb in size, you can use a CD instead of a DVD.

Writing the ISO image to DVD or CD

Before you begin

1. Download any required software from PLDS.
2. Verify that the md5 checksum of the downloaded ISO image matches the md5 checksum that is displayed for the ISO image on the PLDS Web site.

About this task

If you are writing to a DVD, this procedure requires a computer or server that has a DVD writer and software that is capable of writing ISO images to DVD. If you are writing to a CD, this procedure requires a computer or server that has a CD writer and software that is capable of writing ISO images to CD.

Important:

When the ISO image is being written to the DVD, do not run other resource-intensive applications on the computer. Any application that uses the hard disk intensively can cause a buffer underrun or other errors, which can render the DVD useless.

Procedure

Write the ISO image of the installer to a DVD or CD.

Installing System Platform

Installation methods

Use one of the following methods to install System Platform:

- Laptop connected to the services port on the server.
- Video monitor, keyboard, and mouse connected to the appropriate ports on the server.

Note:

You can complete the installation by using only a keyboard and monitor. If you do not have a mouse, use the Tab key to navigate between fields.

If you use a laptop to install the software, you must have an SSH and Telnet client application such as PuTTY installed on the laptop and Telnet must be enabled to install System Platform. Make sure that you change the network settings on the laptop before connecting to the server. See Configuring the laptop for direct connection to the server on page 45.

Server requirements

Server hardware platforms must meet all requirements of the Avaya Aura® System Platform software, any feature-based configuration options (for example, High Availability), and the additional requirements of a specific Avaya Aura® solution template.

Note:

Since each Avaya Aura® solution template has different requirements for server resources, configuration, capacity, and performance, refer to customer documentation specific to the Avaya Aura® solution you are deploying in your network.

Avaya requires that you install each server with an uninterruptible power supply (UPS) unit. The UPS power ratings should exceed server peak power requirements under a sustained maximum processing load. (Consult with Avaya Support at http://support.avaya.com to ensure a reliable installation.)

Installation checklist for System Platform

Use this checklist to guide you through installation of System Platform, the latest available version of the Services Virtual Machine (VM), and SAL Gateway registration and configuration.

Important:

If you are installing with High Availability protection, install the same version of System Platform on the active and standby servers.

No.	Task	Notes	✔
1	If you are installing System Platform from a laptop, perform the following tasks: • Ensure that a Telnet and Secure Shell application are installed on the laptop. Avaya supports use of the open source Telnet/SSH client application PuTTY. • Configure the IP settings of the laptop for direct connection to the server. See Configuring the laptop for direct connection to the server on page 45. • Disable use of proxy servers in the Web browser on the laptop. See Disabling proxy servers in Microsoft Internet Explorer on page 46 or Disabling proxy servers in Mozilla Firefox on page 47 .		
2	If you are installing System Platform from a laptop, connect your laptop to the services port with an Ethernet crossover cable.	If you do not have a crossover cable, use an IP hub. **Note:** Some laptop computer Network Interface Cards (NICs) provide an internal crossover option that makes it possible to use a straight-through Ethernet cable for this connection. See the documentation for your laptop computer to determine	

No.	Task	Notes	✔
		whether this option is available.	
3	If you are installing System Platform from the server console, connect a USB keyboard, USB mouse, and video monitor to the server.		
4	Turn on the server.		
5	Place the DVD in the DVD drive on the server. See Starting the installation from your laptop on page 47 or Starting the installation from the server console on page 48 depending on your selection of installation method.		
6	If using the server console to install System Platform, enter the **`vspmediacheck`** command and press **Enter**. The **`vspmediacheck`** command verifies that the image on the System Platform DVD is not corrupt. See Starting the installation from the server console on page 48.		
7	If using your laptop to install System Platform, establish a Telnet connection to the server. See Starting the installation from your laptop on page 47.		
8	Select the required keyboard type. See Selecting the type of keyboard on page 49.		
9	Verify the System Platform server hardware. See Verifying the System Platform server hardware on page 50.		
10	Verify that the image on the System Platform DVD is not corrupt. See Verifying the System Platform image on the DVD on page 51.		
11	Configure the network settings for the System Domain (Domain-0). See Configuring network settings for System Domain on page 52.		

No.	Task	Notes	✔
12	Configure the network settings for the Console Domain. See Configuring network settings for Console Domain on page 54.		
13	Install the Services Virtual Machine (services_vm). See Installing the Services virtual machine on page 56.	**Important:** When the Services VM Network Configuration window appears at the beginning of the System Platform installation *for the standby server* in a System Platform High Availability configuration, clear the **Enable Services VM** check box to ensure that you install the Services VM in a disabled state. If a failover occurs later during HA system operation, the failover subsystem activates the Services VM on the former standby (now active) server, propagates the current Services VM configuration to that server, and deactivates the Services VM on the former active (now standby) server.	
14	Configure the time zone for the System Platform server. See Configuring the time zone for the System Platform server on page 59.		
15	Configure the date and time and specify an NTP server if using one. See Configuring the date and time for the System Platform server on page 59		
16	Configure the System Platform passwords. See Configuring System Platform passwords on page 60.		
17	Verify that System Platform installed correctly. See Verifying installation of on page 62.		

No.	Task	Notes	✔
18	Check for System Platform patches at http://support.avaya.com. Install any patches that are available. See *Administering Avaya Aura® System Platform* for information on installing patches.		
19	Install a solution template.	**Important:** If you are running System Platform in any of its High Availability modes, do not install a solution template on the standby server. If you do, you will be unable to start High Availability operations. If you are using a bundled System Platform installation (with a solution template), disable template installation on the standby server. Starting High Availability automatically propagates the solution template from the active node to the standby node.	
20	Configure the SAL gateway for remote access and alarming. See SAL Gateway on page 68.		
21	If applicable, configure System Platform High Availability. See Configuring locally redundant High Availability on page 93.		

Connecting your laptop to the server

Configuring the laptop for direct connection to the server

About this task

You must manually configure the IP address, subnet mask, and default gateway of the laptop before you connect the laptop to the server.

Note:

The following procedure is for Microsoft Windows XP, but the steps can vary slightly with other versions of Windows.

Procedure

1. Click **Start** > **Control Panel**.
2. Double-click **Network Connections** > **Local Area Connection**.
3. In the Local Area Connection Status dialog box, click **Properties**.
4. In the **This connection uses the following items** box, click **Internet Protocol (TCP/IP)**.
5. Click **Properties**.
6. In the Internet Protocol (TCP/IP) Properties dialog box, select **Use the following IP address** on the **General** tab.

   ⚠ **Caution:**

   Do not click the **Alternate Configuration** tab.
7. In the **IP address** field, enter a valid IP address.
   For example: `192.11.13.5`
8. In the **Subnet mask** field, enter a valid IP subnet mask.
   For example: 255.255.255.252
9. In the **Default gateway** field, enter the IP address that is assigned to the default gateway.
   For example: `192.11.13.6`
10. Click **OK**.

Disabling proxy servers in Microsoft Internet Explorer

About this task

To connect directly to the services port, disable the proxy servers in Internet Explorer.

Procedure

1. Start Internet Explorer.
2. Select **Tools** > **Internet Options**.
3. Click the **Connections** tab.
4. Click **LAN Settings**.
5. Clear the **Use a proxy server for your LAN** option.

   ⊕ **Tip:**

   To reenable the proxy server, select the **Use a proxy server for your LAN** option again.

6. Click **OK** to close each dialog box.

Disabling proxy servers in Mozilla Firefox

About this task

To connect directly to the services port, disable the proxy servers in Firefox.

Note:

This procedure is for Firefox on a Windows-based computer. The steps can vary slightly if you are running Linux or another operating system on your laptop.

Procedure

1. Start Firefox.
2. Select **Tools** > **Options**.
3. Select the **Advanced** option.
4. Click the **Network** tab.
5. Click **Settings**.
6. Select the **No proxy** option.

   Tip:

   To reenable the proxy server, select the appropriate option again.
7. Click **OK** to close each dialog box.

Starting the installation

Starting the installation from your laptop

Before you begin

- A Telnet/SSH application, such as PuTTY, is installed on your laptop.
- IP settings of the laptop are configured for direct connection to the server.
- Use of proxy servers is disabled.

Procedure

1. Connect your laptop to the services port with an Ethernet crossover cable.

   If you do not have a crossover cable, use an IP hub.

   Note:

   Some laptop computer Network Interface Cards (NICs) provide an internal crossover option that makes it possible to use a straight-through Ethernet cable for this connection. See the documentation for your laptop computer to determine whether this option is available.

2. Turn on the server.
3. Insert the System Platform DVD in the server DVD drive.
   The server boots from the DVD.
4. Verify that the laptop can ping the service port by performing the following steps:
   a. Click **Start** > **Run**.
   b. Enter `ping -t` *`IP_Address`*.
   For example: `ping -t 192.11.13.6`

   Note:

   Wait for the `ping` command to return several continuous responses before proceeding to the next step.
5. Open a Telnet session by performing the following steps:

   Important:

   If you use a Telnet client other than PuTTY or forget to set the proper terminal emulation for the PuTTY client, the system could display an incorrect Keyboard Type. This issue has no effect on the installation process.

   a. Open the PuTTY application.
   b. In the **Host Name** field, enter *Host_Name*.
   For example: `192.11.13.6`
   c. Under **Connection type**, select **Telnet**.
   d. Under **Window** in the left navigation pane, select **Translation**.
   e. Under **Received data assumed to be in which character set** , select **UTF-8** from the list.
   f. Click **Open** to open a PuTTY session.

   The system displays the Keyboard Type screen.

Next steps

Select the required keyboard type. See Selecting the type of keyboard on page 49.

Related topics:

Connecting to the server through the services port on page 64

Starting the installation from the server console

Before you begin

Connect a USB keyboard, USB mouse, and video monitor to the server.

Procedure

1. Turn on the server.
2. Insert the System Platform DVD in the server DVD drive.
   The server boots up from the System Platform DVD and displays the Avaya screen.
3. Within 30 seconds of the system displaying the Avaya screen, type **`vspmediacheck`** at the boot prompt on the Avaya screen, and press **Enter**.

   The **`vspmediacheck`** command verifies that the image on the System Platform DVD is not corrupt.

   > ❗ **Important:**
   >
   > If you do not press **Enter** or type **`vspmediacheck`** within 30 seconds of the system displaying the Avaya screen, the system disables installation through the server console and enables installation through the services port. The system then displays the Waiting for Telnet connection screen, and then you can connect to the server through Telnet. To install through the server console at this point, reset the server to restart the installation.

   The system displays the Keyboard Type screen.

Next steps

Select the required keyboard type. See Selecting the type of keyboard on page 49.

Selecting the type of keyboard

Procedure

1. On the Keyboard Type screen, select the type of keyboard that you have.

   The supported keyboard types are sg-latin1, sk-qwerty, slovene, sv-latin1, trq, ua-utf, uk, and us.
2. Use the `Tab` key to highlight **OK** and press **Enter**.
   The system displays one of the following screens:
   - The system displays the CD Found screen if you are installing System Platform from a laptop, or if you are installing System Platform from the server console and entered the **`vspmediacheck`** command at the boot prompt on the Avaya screen.

     See Verifying the System Platform image on the DVD on page 51.
   - The system displays the System Domain Network Configuration screen if you are installing System Platform from the server console and did not enter the

vspmediacheck command at the boot prompt on the Avaya screen. See Configuring network settings for System Domain (Domain-0) on page 52.

Next steps

- Verify that the System Platform image was copied correctly to the DVD. See Verifying the System Platform image on the DVD on page 51.

  OR
- Configure the network settings for System Domain (Domain-0). See Configuring network settings for System Domain (Domain-0) on page 52

Verifying the System Platform server hardware

Before you begin

- You are performing a new installation of the System Platform software.
- You have just completed the task, Selecting the type of keyboard on page 49

About this task

After Selecting the type of keyboard on page 49, the System Platform installer automatically performs a hardware check of the server platform. Since the servers supported by Avaya must meet all prerequisites for the System Platform , any platform options, and a specific solution template, the server hardware check normally passes. In this case, the System Platform installation proceeds transparently to the next phase, Verifying the System Platform image on the DVD on page 51. However, in the rare circumstance when the hardware check halts the System Platform installation, one or both of the following messages appear. (In the following examples, the first number represents what hardware resources the system nominally requires, and the second number represents what hardware resources the server actually has available for the system.)

```
The installation is going to abort due to the following reasons:

  • The expected minimum size of hard disk is 80 GB, but the actual
    number of hard disk is 40 GB.

  • The expected number of hard disk is 2, but the actual number of
    hard disk is 1.
```

Or:

```
The installer has detected the following problems:

 • The expected number of CPU(s) is 2, but the actual number of CPU(s)
   is 1.

Do you still want to continue the installation?
```

In either case, capture the exact details of the error message and contact your Avaya technical support representative for further instructions.

Note:

For any instance of the latter message, do not continue with the System Platform installation.

Next steps

If the server hardware check passed, continue with Verifying the System Platform image on the DVD on page 51

Verifying the System Platform image on the DVD

About this task

Use this procedure to verify that the System Platform image was copied correctly to the DVD.

The system displays the CD Found screen if you are installing System Platform from a laptop, or if you are installing System Platform from the server console and entered the **`vspmediacheck`** command at the boot prompt on the Avaya screen.

Procedure

On the CD Found screen, perform one of the following actions:

- To test the DVD, use the `Tab` key to select **OK**.
- To skip the test and begin the installation immediately, select **Skip**.

If you choose to test the DVD, the system displays another screen with a progress bar and the percentage of completion. After the test is complete, the system displays whether the image passed the test.

Note:

If the DVD you are using is corrupt, you must write a new DVD with the System Platform image. Before using the new DVD, make sure that you restart the server.

The system displays the System Domain Network Configuration screen.

Next steps

Configure the network settings for System Domain (Domain-0). See Configuring network settings for System Domain (Domain-0) on page 52.

Related topics:

Writing the ISO image to DVD or CD on page 40

Configuring network settings for System Domain

Procedure

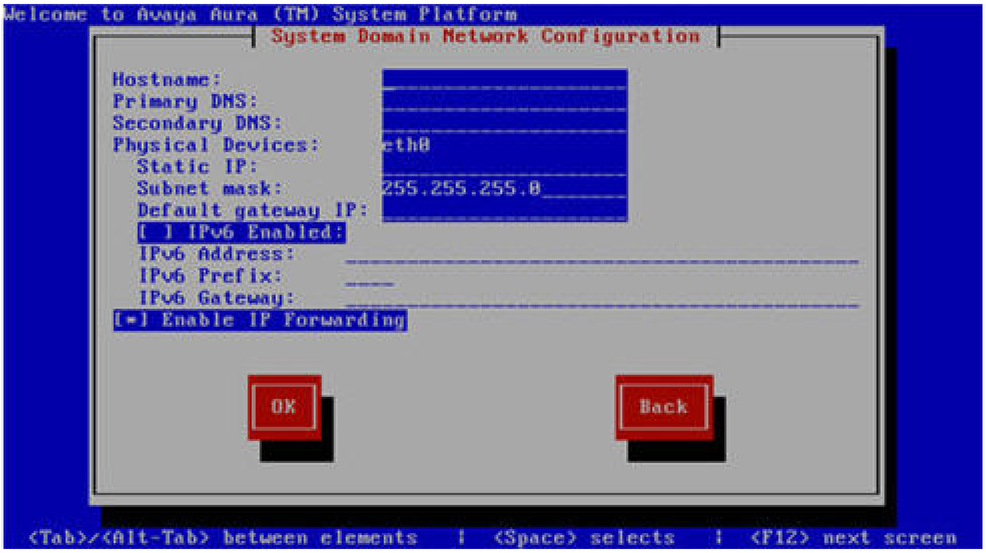
1. On the System Domain Network Configuration screen, complete the following fields:

    - **Hostname**

      Depending on requirements of your solution template, you might need to enter the host name for System Domain as a fully qualified domain name (FQDN), for example, `SPDom0.mydomainname.com`. Otherwise, just enter the IP address for System Domain, or enter the hostname for System Domain in non-FQDN format. When using a Domain Name System (DNS) server in your network, the System Domain hostname must be FQDN format.

    - **Primary DNS**
    - (Optional) **Secondary DNS**

    For descriptions of the fields on this page, see System Domain Network Configuration field descriptions on page 53.



```
Welcome to Avaya Aura (TM) System Platform
              System Domain Network Configuration

Hostname:
Primary DNS:
Secondary DNS:
Physical Devices:          eth0
  Static IP:
  Subnet mask:             255.255.255.0
  Default gateway IP:
  [ ] IPv6 Enabled:
  IPv6 Address:
  IPv6 Prefix:
  IPv6 Gateway:
[*] Enable IP Forwarding
```

OK
Back
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

2. Perform the following steps to configure the interface that is connected to the customer network:

    a. Use the `Tab` key to highlight the **Physical Devices** field.

    b. Complete the **Static IP** field.

    c. Modify the subnet mask if necessary. The server displays a default value of 255.255.255.0.

3. Complete the **Default gateway IP** field.

4. Use the Tab key to highlight the **IPv6 Enabled** field. Press the Spacebar to either enable or disable entering IP addresses in IPv6 format.
5. If you have enabled IPv6, fill in the following fields:
   - **IPv6 Address**
   - **IPv6 Prefix**
   - **IPv6 Gateway**
6. Use the Tab key to highlight the **Enable IP Forwarding** field. Press the Space bar to either enable or disable the IP forwarding as desired.

   Note:

   IP forwarding is enabled by default and is denoted by an asterisk (* character).
7. Use the Tab key to highlight **OK** and press **Enter** to accept the configuration.
8. If IP forwarding is enabled, a confirmation message is displayed. Use the Tab key to highlight **OK** and press **Enter**.
   The system displays the System Platform Console Domain Network Configuration screen.

Next steps

Configure network settings for Console Domain. See Configuring network settings for Console Domain on page 54.

System Domain Network Configuration field descriptions

Name	Description
Hostname	Depending on requirements of your solution template, you might need to enter the host name for System Domain as a fully qualified domain name (FQDN), for example, SPDom0.mydomainname.com. Otherwise, just enter the IP address for System Domain, or enter the hostname for System Domain in non-FQDN format. When using a Domain Name System (DNS) server in your network, the System Domain hostname must be FQDN format.
Primary DNS	The primary Domain Name System (DNS) server address.
Secondary DNS	(Optional) The secondary DNS server address.
Physical Devices	This field displays the physical Ethernet interface (NIC) that connects to the customer

Name	Description
	network. You must configure this interface for IP. The specific Ethernet interface number depends on the server model being used.
Static IP	The static IP address for the Ethernet interface that connects to the customer network.
Subnet Mask	The subnet mask for the Ethernet interface that connects to the customer network.
Default gateway IP	The default gateway IP address. This default gateway IP address will be used for all the virtual machines if you do not specify gateway IP addresses for them.
IPv6 Enabled	The indicator to show whether the IP addresses required by System Platform must be IPv6-compliant.
IPv6 Address	The IPv6-compliant IP address of System Domain.
IPv6 Prefix	The IPv6 prefix for **IPv6 Address**.
IPv6 Gateway	The IP address of the default gateway for IPv6 traffic.
Enable IP Forwarding	The indicator to show whether IP forwarding is enabled. An asterisk on the left of the field denotes that IP forwarding is enabled. IP forwarding enables access through the services port to virtual machines on System Platform, including System Domain and Console Domain. IP forwarding must be enabled for both SSH and Web Console access.

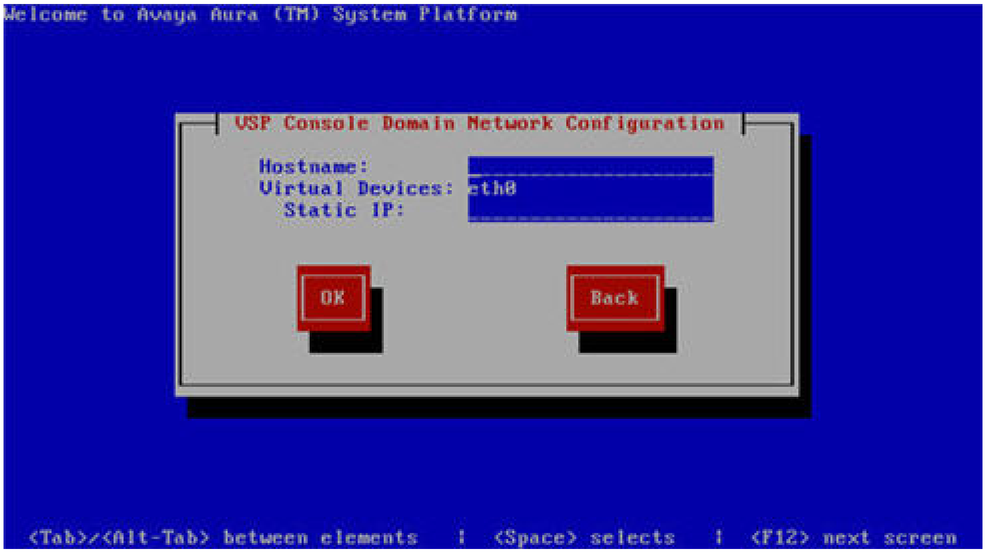
Configuring network settings for Console Domain

Procedure

1. On the VSP Console Domain Network Configuration screen, complete the following fields to set up the Console Domain network:
   - **Hostname**.

     Depending on requirements of your solution template, you may need to enter the host name for Console Domain as a fully qualified domain name (FQDN), for example, `SPCdom.mydomainname.com`. Otherwise, just enter the IP address for Console Domain or enter the hostname for Console Domain in non-FQDN format.

- **Static IP**



Welcome to Avaya Aura (TM) System Platform

VSP Console Domain Network Configuration

Hostname:
Virtual Devices: eth0
Static IP:

OK
Back
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

2. Select **OK** and press **Enter** to accept the configuration and display the Services VM Network Configuration screen.

Next steps

Install and configure the Services Virtual Machine. See Installing the Services virtual machine on page 56.

System Platform Console Domain Network Configuration field descriptions

Name	Description
Hostname	Depending on requirements of your solution template, you may need to enter the host name for Console Domain as a fully qualified domain name (FQDN), for example, `SPCdom.mydomainname.com`. Otherwise, just enter the IP address for Console Domain or enter the hostname for Console Domain in non-FQDN format.
Static IP	The IP address for the Console Domain. **Note:** The Console Domain does not have a physical interface. It has a virtual interface that uses the physical interface in System Domain (Domain-0). Because System Domain acts like a bridge, the IP address

Name	Description
	that you enter here must be a valid IP address. Further, the Console Domain must be on the same network as System Domain (Domain-0).
Virtual Devices	The virtual device (port) assigned to the Console Domain (Cdom) virtual machine. Default value (eth0) automatically assigned. No user input necessary.

Installing the Services virtual machine

Beginning with System Platform release 6.2, the Secure Access Link Gateway (SAL Gateway) no longer runs on the System Platform Console Domain (cdom) virtual machine. Instead, SAL Gateway runs on an independent Services virtual machine (services_vm domain) on your Avaya Aura® solution server. As with the prior implementation of the SAL Gateway running on the cdom virtual machine, this new configuration supports secure remote access to local server resources, and forwards alarms (SNMP traps) from your local solution server to a remote Network Management System (NMS).

Releases of the Services virtual machine are independent of System Platform releases, so your system may use the existing Services VM 2.0, or you can subsequently upgrade your system to use a later version of the Services VM. When you upgrade the Services VM, the process preserves the prior Master Agent configuration. For information about how to upgrade the Services VM, see *Implementing and Administering Services-VM on Avaya Aura® System Platform*, which is available from Avaya Support at http://support.avaya.com. After the upgrade, you configure the Net-SNMP Master Agent in Services VM to forward either SNMPv2c or SNMPv3 traps to your NMS.

For *new System Platform installations* (not an upgrade procedure), you must install the Services virtual machine as part of the platform installation process. An exception to this requirement occurs when implementing a centralized SAL system, with the SAL Gateway running on a separate, dedicated server elsewhere in your network. In this case, you disable Services virtual machine installation during installation of System Platform.

Important:

When the Services VM Network Configuration window appears at the beginning of the System Platform installation *for the standby server* in a System Platform High Availability configuration, clear the **Enable Services VM** check box to ensure that you install the Services VM in a disabled state. If a failover occurs later during HA system operation, the failover subsystem activates the Services VM on the former standby (now active) server, propagates the current Services VM configuration to that server, and deactivates the Services VM on the former active (now standby) server.

For platform upgrades (not a new System Platform installation), the platform upgrade process manages installation of the new Services VM and SAL Gateway transparently except where an administrator must enter configuration values.

For more information about SAL capabilities, see *Secure Access Link 2.2 SAL Gateway Implementation*, at http://support.avaya.com.

Before you begin

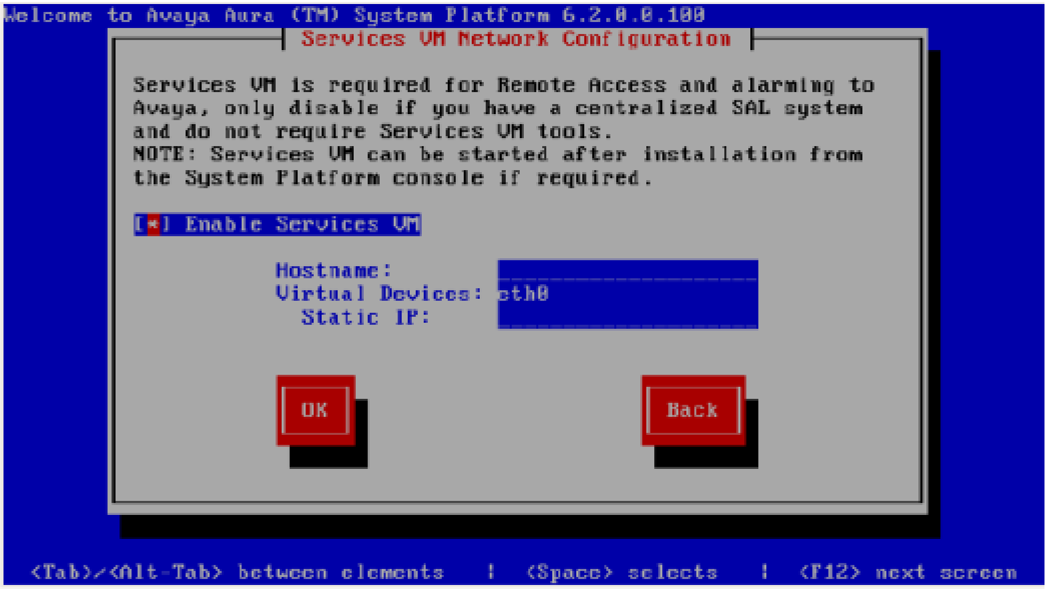
- You have just completed the task, “Configuring network settings for Console Domain.”
- If you plan to deploy a stand-alone SAL Gateway on a server elsewhere in your network, you must download, install, and configure the SAL 2.2 software on that server. For instructions, see the SAL Gateway installation section of *Avaya Secure Access Link 2.2 Gateway Implementation*, available at the Avaya Support Web site at http://support.avaya.com.

About this task

Use this procedure to install the Services VM in an enabled or disabled state, when the Services VM Network Configuration window appears during System Platform installation .

Procedure

1. If you have a separate server dedicated for centralized SAL support, clear the **Enable Services VM** option in the Services VM Network Configuration window and click **OK**. Otherwise, leave the **Enable services VM** option enabled and begin with step 2 on page 57.
   If you disable the **Enable Services VM** option, System Platform installation automatically proceeds to “Configuring System Platform time to synchronize with an NTP server.”
2. In the Services VM Network Configuration window, enter a **Hostname** for the Services virtual machine.



```
Welcome to Avaya Aura (TM) System Platform 6.2.0.0.100
Services VM Network Configuration

Services VM is required for Remote Access and alarming to
Avaya, only disable if you have a centralized SAL system
and do not require Services VM tools.
NOTE: Services VM can be started after installation from
the System Platform console if required.

[*] Enable Services VM

Hostname:
Virtual Devices: eth0
Static IP:

<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen
```

3. Enter a **Static IP** address for the Services virtual machine.

   The IP address must be on the same subnet assigned to the Domain 0 (dom0) and Console Domain (cdom) virtual machines.

4. Click **OK**.
   The Time Zone Selection screen is displayed.

Next steps

Configure the time zone for the server.

Related topics:

Services VM Network Configuration field descriptions on page 58

Services VM Network Configuration field descriptions

Name	Description
Enable Services VM	Enables or disables remote access. Also supports local or centralized alarm reporting. Default value: **Enabled** Leave the **Enable services VM** option enabled (check mark) for remote access and local SAL support, or disabled (no check mark) if you have a separate server dedicated for independent/centralized remote access and SAL support. In a System Platform High Availability configuration, the active node automatically propagates to the standby node, any change in the setting for this field
Hostname	The name you assign to the Services virtual machine.
Static IP address	The IP address you assign to the Services virtual machine. The address must be on the same subnet assigned to the Domain 0 (dom0) and Console Domain (cdom) virtual machines.
Virtual devices	The virtual device (port) assigned to the Services virtual machine. Default value (eth0) automatically assigned. No user input necessary.

Configuring the time zone for the System Platform server

Procedure

1. On the Time Zone Selection screen, select the time zone in which the server is located.
2. Select **OK** and press **Enter** to accept the configuration and display the Date/Time and NTP setup screen.

Next steps

Configure date and time for the server.

Configuring the date and time for the System Platform server

About this task

For solution templates supporting the Network Time Protocol (NTP), the use of an NTP server within your network is the preferred configuration for synchronizing System Platform server time to a standards-based NTP time source. Otherwise, manually configure the System Platform server to a local time setting.

Procedure

1. Set the current date and time on the Date/Time and NTP setup screen.

   Note:

   Ensure that the time set here is correct upon initial installation. Changing the time in a virtual machine environment causes virtual machines to reboot.

2. If you are using an NTP server, perform the following steps on the Date/Time and NTP setup screen:

   a. Select **Use NTP** if you are using one or more NTP servers.

   b. In the **NTP server** fields, enter the DNS name or the IP address of your preferred NTP servers.

3. Select **OK** and press **Enter** to accept the configuration and display the Passwords screen.

Next steps

Configure System Platform passwords.

Configuring System Platform passwords

Before you begin

Configure the date and time for the System Platform server.

About this task

Important:

The customer is responsible for the security of all system passwords including the password for the root account. The root password on System Domain must be kept very secure. This account has a very high level of access to the system and steps should be taken to ensure that the password is known only to authorized users. Incorrect use of the root login can result in serious system issues. The root account must be used only in accordance with Avaya documentation and when instructed to do so by Avaya Services.

Procedure

1. On the Passwords screen, enter new passwords for all logins. You must enter each password twice to ensure that you are not making any mistakes in typing.

   If you do not enter new passwords, the defaults are used. The following table shows the default password for each login.

Login	Default password	Capability
root	root01	Advanced administrator
admin	admin01	Advanced administrator
cust	cust01	Normal administrator
manager (for ldap)	root01	Administrator for the System Platform local Lightweight Directory Access Protocol (LDAP) directory. System Platform uses a local LDAP directory to store login and password details. Use this login and password to log in to the local LDAP directory. This login does not have permissions to access the System Platform Web Console.

Important:

Enter new passwords instead of using the default passwords. Exercising best practice for password security, make careful note of the passwords that you set for all logins. Customers are responsible for managing their passwords.

Passwords for all users including `root` must adhere to the following rules:

- Include a minimum of 8 characters.
- Include no more than five repeating characters.
- Cannot include the last password as part of a new password.
- Cannot include the user ID as part of the password.
- Cannot be changed more than once a day.

Note:

The Avaya Services craft login uses Access Security Gateway (ASG) for authentication. If you are using the craft login, you must have an ASG tool to generate a response for the challenge that is generated by the login page. Many ASG tools are available such as Avaya Token Mobile, Avaya Web Mobile, and Site Manager. The first two ASG tools must be able to reach the ASG manager servers behind the Avaya firewall. The Avaya Services representative uses Site Manager to pull the keys specific to a site before visiting that site. At the site, the Avaya Services representative uses those keys to generate a response for the challenge generated by the Logon page.

2. Select **OK** and press **Enter** to accept the passwords and continue the installation.

Result

The installation takes approximately 5 minutes. During this time, you can see the Image Installation page with progress bars, followed by the Running page, as the system completes the post-install scripts. After the installation is completed, the system ejects the DVD and reboots the server. If you are installing from server console, the system displays the Linux login page for System Domain (Domain-0) after the reboot.

Important:

If the DVD does not eject automatically, eject it manually. The system restarts the installation if the DVD is not ejected.

Caution:

Do not shut down or reboot the server during the first boot process of Console Domain. If you shutdown or reboot the server during the first boot of Console Domain, System Platform will not function correctly and will have to be reinstalled. To determine if Console Domain has booted, attempt to access the Web Console. See Accessing the Web Console on page 65.

Next steps

Verify System Platform installation. See Verifying installation of on page 62.

Passwords field descriptions

Note:

Passwords for all users including `root` must adhere to the following rules:

- Include a minimum of 8 characters.
- Include no more than five repeating characters.
- Cannot include the last password as part of a new password.
- Cannot include the user ID as part of the password.
- Cannot be changed more than once a day.

Name	Description
root Password	The password for the root login.
admin Password	The password for the admin login.
cust Password	The password for the cust login.
ldap Password	The password for the ldap login. System Platform uses a local LDAP directory to store login and password details. Use this login and password to log in to the local LDAP directory. This login does not have permissions to access the System Platform Web Console.

Verifying installation of System Platform

Before you begin

To gain access to the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 65.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

After installing System Platform, use this procedure to successfully log on to:

- The System Domain (Dom0) command line as `root`, and run the **`check_install`** command.
- The Console Domain (Cdom) Web Console as `admin`.
- The Console Domain as `cust`.

Note:

The System Platform installation program installs the Console Domain after installing the System Domain. Availability of the login prompt for the System Domain does not necessarily mean that the Console Domain was installed successfully.

The actions in this procedure collectively help to verify successful installation of System Platform, and identify various issues associated with an unsuccessful installation, as well.

Procedure

1. Access the System Domain command line.

   See Accessing the command line for System Domain on page 66.

2. Enter the command, **`check_install`**.
   If **`check_install`** finds no issues, the following message appears in the command line interface:

   ```
   Cursory checks passed.
   ```

   If **`check_install`** command indicates a problem, wait a few minutes and run the command again. If the problem persists, contact Avaya using any of the technical support options at http://support.avaya.com.

3. Type **`exit`** to exit root login.

4. Type **`exit`** again to exit the System Domain.

5. Access the System Platform Web Console. See Accessing the Web Console on page 65.

6. Perform the following steps to log in to Console Domain as `admin`:

   a. Start PuTTY from your computer.
   b. In the **Host Name (or IP Address)** field, type the IP address of Console Domain.
   c. In the **Connection type** field, select **SSH**, and then click **Open**.
   d. When prompted, log in as `admin`, and type the password that you entered for the admin login during System Platform installation.
   e. Type `exit` to exit Console Domain.

7. Perform the following steps to log in to Console Domain as `cust`:

   a. Start PuTTY from your computer.
   b. In the **Host Name (or IP Address)** field, type the IP address of Console Domain.

c. In the **Connection type** field, select **SSH**, and then click **Open**.

d. When prompted, log in as `cust`, and type the password that you entered for the cust login during System Platform installation.

e. Type `exit` to exit Console Domain.

Important:

If you cannot log in to Console Domain as `admin` or `cust` or access the System Platform Web Console, contact Avaya using any of the technical support options at http://support.avaya.com.

Accessing System Platform

Connecting to the server through the services port

Before you begin

- A Telnet/SSH application, such as PuTTY, is installed on your laptop.
- IP settings of the laptop are configured for direct connection to the server.
- Use of proxy servers is disabled.

Procedure

1. Connect your laptop to the services port with an Ethernet crossover cable.

   If you do not have a crossover cable, use an IP hub.

   Note:

   Some laptop computer Network Interface Cards (NICs) provide an internal crossover option that makes it possible to use a straight-through Ethernet cable for this connection. See the documentation for your laptop computer to determine whether this option is available.

2. Start a PuTTY session.
3. In the **Host Name (or IP Address)** field, type `192.11.13.6`.

   The system assigns the IP address 192.11.13.6 to the services port.

4. For **Connection type**, select **SSH**.
5. In the **Port** field, type `22`.
6. Click **Open**.

   Note:

   The system displays the PuTTY Security Alert window the first time you connect to the server.

7. Click **Yes** to accept the server's host key and display the PuTTY window.
8. Log in as **admin** or another valid user.
9. When you finish the session, type `exit` and press **Enter** to close PuTTY.

Related topics:

Configuring the laptop for direct connection to the server on page 45
Disabling proxy servers in Microsoft Internet Explorer on page 46
Disabling proxy servers in Mozilla Firefox on page 47

Enabling IP forwarding to access System Platform through the services port

About this task

To gain access to virtual machines on System Platform by connecting a laptop to the services port, you must enable IP forwarding on System Domain (Domain-0). Enable IP forwarding to gain access to both SSH and Web Console.

You can set the IP forwarding status to enabled or disabled during System Platform installation. The system enables IP forwarding by default. To enable or disable IP forwarding, use the following procedure.

Note:

For security reasons, always disable IP forwarding after finishing your task.

Procedure

1. To enable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as administrator.
   c. In the command line, type `ip_forwarding enable` and press **Enter**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to System Domain (Domain-0) as administrator.
   c. In the command line, type `ip_forwarding disable` and press **Enter**.

      An alternative to the above command is `service_port_access disable`.

Accessing the System Platform Web Console

Before you begin

To gain access to the System Platform Web Console from a laptop that is connected to the services port, enable IP forwarding. See Enabling IP forwarding to access through the services port on page 65.

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

You can access the System Platform Web Console from a Web browser on your laptop or another computer connected to the same network as the System Platform server.

Procedure

1. Open a compatible Internet browser on your computer.

   Currently, System Platform supports Internet Explorer 7 and 8, and Firefox 3.6 through 15.0.1.

2. Type the URL: `https://`*`ipaddress`*, where *ipaddress* is the IP address of the Console Domain that you configured during installation of System Platform.

   Note:

   This is a secure site. If you get a certificate error message, follow the instructions on your browser to install a valid certificate on your computer.

3. Enter a valid user ID.
4. Click **Continue**.
5. Enter a valid password.
6. Click **Log On**.

   The system displays the License Terms page when you log in for the first time.

7. Click **I Accept** to accept the end-user license agreement.

   The system displays the Virtual Machine List page in the System Platform Web Console.

Related topics:

Enabling IP forwarding to access System Platform through the services port on page 65

Accessing the command line for System Domain

About this task

If you have physical access to the system, you can log in to the system directly. When you connect to the services port, you are connected to System Domain. Alternatively, use an SSH (Secure Shell) client such as PuTTY to set up a remote connection from your computer. After logging in, the system prompts you with the Linux command prompt.

Note:

Administrators access the command line for System Domain to perform a very small number of tasks. Access to the command line for System Domain is normally reserved only for Avaya or Avaya Partners for troubleshooting purposes.

Procedure

1. Start PuTTY from your computer.
2. In the **Host Name (or IP Address)** field, type the IP address of System Domain.

   Tip:

   You can obtain the IP address of System Domain (Domain-0) from the Virtual Machine Management page of the Web Console. In the navigation pane of the Web Console, click **Virtual Machine Management** > **Manage**.
3. In the **Connection type** field, select **SSH**, and then click **Open**.
4. When prompted, log in as `admin`.
5. Once logged in, type the following command to log in as the root user: `su — root`
6. Enter the password for the *root* user.

   Tip:

   To access Console Domain from System Domain, type **`xm list`**, note the ID for *udom*, and then type **`xm console`** *`udom-id`*. When prompted, login as `admin`. Then type **`su — root`** and enter the root password to log in as root.

   To exit Console Domain and return to System Domain, press `Control+]`.
7. After performing the necessary tasks, type `exit` to exit root login.
8. Type `exit` again to exit System Domain.

Accessing the command line for Console Domain

About this task

Important:

You cannot gain access to Console Domain until the system finishes the first boot process.

Note:

Administrators access the command line for Console Domain to perform a very small number of tasks. Access to the command line for Console Domain is normally reserved only for Avaya or Avaya Partners for troubleshooting purposes.

Procedure

1. Start PuTTY from your computer.
2. In the **Host Name (or IP Address)** field, type the IP address of Console Domain.

   ⊕ **Tip:**

   The IP address of Console Domain (cdom) is the same as the IP address of the System Platform Web Console.
3. In the **Connection type** field, select **SSH**, and then click **Open**.
4. When prompted, log in as `admin`.
5. Once logged in, type the following command to log in as the root user: `su — root`
6. Enter the password for the *root* user.
7. After performing the necessary tasks, type `exit` to exit root login.
8. Type `exit` again to exit Console Domain.

Configuring SAL Gateway on System Platform

SAL Gateway

Secure Access Link (SAL) Gateway provides Avaya support engineers and Avaya Partners with alarming and remote access to the applications on System Platform. System Platform includes an embedded SAL Gateway. SAL Gateway software is also available separately for stand-alone deployments. The SAL Gateway application on System Platform receives alarms from applications in the solution template and forwards them to Secure Access Core Concentrator Servers at Avaya and applicable Avaya Partners. SAL Gateway can also forward alarms to the customer's Network Management System (NMS) if configured to do so. The SAL gateway application also polls designated service providers for connection requests.

Remote Serviceability

System Platform utilizes SAL as Avaya’s exclusive method for remote delivery of services. System Platform can be serviced remotely, possibly eliminating a service technician visit to the customer site. System Platform uses the customer’s existing Internet connectivity to facilitate remote support. All communication is outbound from the customer’s environment using encapsulated Hypertext Transfer Protocol Secure (HTTPS). SAL requires upload bandwidth (customer to Avaya or Avaya Partner) of at least 90 KB/s with latency no greater than 150 ms (round trip). Business Partners without a SAL Core Concentrator Server must provide their own IP-based connectivity (for example, B2B VPN connection) to deliver remote services.

Note:

Avaya Partners and customers must register SAL at least three weeks prior to activation during System Platform installation. Avaya support will be delayed or not possible if SAL is improperly implemented or not operational. System Platform and SAL do not support modem connections.

Stand-alone SAL Gateway

You can choose to use a stand-alone SAL Gateway instead of the SAL Gateway that is embedded in System Platform. You might prefer a stand-alone gateway if you have a large network with many Avaya devices. The stand-alone gateway makes it possible to consolidate alarms from many Avaya devices and send those alarms from one SAL Gateway rather than multiple SAL Gateways sending alarms. See **Secure Access Link** on http://support.avaya.com for more information on stand-alone SAL Gateway.

If you use a stand-alone SAL Gateway, you must add it as an SNMP trap receiver for System Platform. See Adding an SNMP trap receiver on page 84. You can also disable the SAL Gateway that is embedded in System Platform so that it does not send duplicate heart beat messages to Avaya. See Disabling SAL Gateway on page 85.

SAL Gateway configuration

The SAL Gateway includes a Web-based user interface that provides status information, logging information, and configuration interfaces. You must configure the SAL Gateway and other devices for alarming and remote access. The devices include System Platform's System Domain (dom 0), Console Domain (cdom), and other products that are included in the solution template that is installed. For example, virtual machines might include Communication Manager, Communication Manager Messaging, Session Manager, and other applications that are included in the template.

To configure SAL, perform these high-level steps:

1. Register the system.

   You must submit the Universal Install/SAL Registration Request form to obtain from Avaya the information that you must enter in SAL Gateway.

   Avaya assigns a Solution Element ID (SE ID) and Product ID to each SAL Gateway and managed device that is registered. In the context of System Platform, managed devices are the components of System Platform and of the applications that are included in the solution template. The SE ID makes it possible for Avaya Services or Avaya Partners to connect to the managed applications remotely. The Product ID is included in alarms that are sent to alarm receivers from the managed device. The Product ID identifies the device that generated the alarm. This data is critical for correct execution of various Avaya business functions and tools.

2. Configure the SAL Gateway.

   The SAL Gateway provides remote access to those devices that are configured for remote access within it. It controls connections to managed elements, new or updated models, and verifies certificates for authentication.

Note:

On systems using High Availability operation, configure the SAL Gateway only on the primary server. When you enable High Availability operations, SAL Gateway will propagate to the standby server.

Related topics:

Registering the system on page 36

Configuration prerequisites on page 70

Configuration prerequisites

Before configuring the SAL Gateway, you must start the registration process and receive product registration information from Avaya.

To register a product, download and complete the *Universal Install/SAL Registration Request* form and submit the form to Avaya. The form includes complete instructions. Open the Microsoft Excel form with macros enabled.

This form is available at http://support.avaya.com. In the navigation pane, click **More Resources** > **Avaya Equipment Registration**. Under Non-Regional (Product) Specific Documentation, click **Universal Install/SAL Product Registration Request Form**, or search *Universal Install/SAL Product Registration Request Form*.

Note:

Submit the registration form three weeks before the planned installation date.

Related topics:

Registering the system on page 36

SAL Gateway on page 68

Changing the Product ID for System Platform

Before you begin

You must have registered the system and obtained a Product ID for System Platform from Avaya. The Product ID is included in alarms that System Platform sends to alarm receivers. The Product ID identifies the device that generated the alarm. This data is critical for correct execution of various Avaya business functions and tools.

About this task

When you install System Platform, a default Product ID of 1001119999 is set. You must change this default ID to the unique Product ID that Avaya provides.

Procedure

1. In the navigation pane of the System Platform Web Console, click **Server Management** > **SNMP Trap Receiver Configuration**.
2. On the SNMP Trap Receiver Configuration page, delete the ID that is displayed in the **Product ID** field and enter the unique Product ID for System Platform Console Domain.

   Note:

   VSPU is the model name for Console Domain.
3. Click **Save**.

System and browser requirements

Browser requirements for accessing the SAL Gateway user interface:

- Internet Explorer 7 or 8
- Firefox 3.6 through 15.0.1

System requirements:

- A computer with access to the System Platform network.

Starting the SAL Gateway user interface

Procedure

1. Log in to the System Platform Web Console.
2. In the navigation pane of the System Platform Web Console , click **Server Management** > **SAL Gateway Management**.
3. On the **Server Management: SAL Gateway Management** page, click **Enable SAL Gateway**.
4. On the SAL Gateway Management page, click **Launch SAL Gateway Management Portal**.
5. When the SAL Gateway displays its Log on page, enter the same user ID and password that you used for the System Platform Web Console.

   To configure SAL Gateway, you must log in as `admin` or another user that has an advanced administrator role. Users that have an administrator role can only view configuration of the SAL Gateway.

When you are successfully logged in, the Managed Element page of the SAL Gateway user interface is displayed. If the SAL Gateway is up and running, the system displays two messages at the top of the page:

- `SAL Agent is running`
- `Remote Access Agent is running`

Configuring the SAL Gateway

About this task

Use this procedure to configure the identity of the SAL Gateway. This information is required for the SAL Gateway to communicate with the Secure Access Concentrator Core Server (SACCS) and Secure Access Concentrator Remote Server (SACRS) at Avaya.

Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Gateway Configuration**.
2. On the Gateway Configuration page, click **Edit**.
3. On the **Gateway Configuration** (edit) page, complete the following fields:
    - **IP Address**
    - **Solution Element ID**
    - **Alarm ID**
    - **Alarm Enabled**

   For field descriptions, see Gateway Configuration field descriptions on page 73.
4. (Optional) Complete the following fields if the template supports inventory collection:
    - **Inventory Collection**
    - **Inventory collection schedule**
5. Click **Apply**.

   Note:

   The configuration changes do not take effect immediately. The changes take effect after you apply configuration changes on the Apply Configuration Changes page.
6. If necessary to cancel your changes, click **Undo Edit**.

   The system restores the configuration before you clicked the **Edit** button.

See the *Secure Access Link Gateway 2.2 Implementation Guide* for more information. This document is available at http://support.avaya.com.

Next steps

After completing configuration of SAL Gateway, you must apply configuration changes for the configuration to take effect. This task is performed on the Apply Configuration Changes page and restarts the SAL Gateway. To minimize disruption of services and alarms, apply configuration changes only after you finish configuration of SAL Gateway.

Related topics:

Gateway Configuration field descriptions on page 73

Applying configuration changes on page 81

Gateway Configuration field descriptions

Name	Description
Hostname	A host name for the SAL Gateway. ⚠ **Warning:** Do not edit this field as the SAL Gateway inherits the same hostname as the CentOS operating system that hosts both the System Platform Web Console and the SAL Gateway.
IP Address	The IP address of the SAL Gateway. This IP address must be different from the unique IP addresses assigned to either the Cdom or Dom0 virtual machines.
Solution Element ID	The Solution Element ID that uniquely identifies the SAL Gateway. Format is `(000)123-4567`. If you have not obtained Solution Element IDs for the system, start the registration process. The system uses the SAL Gateway Solution Element ID to authenticate the SAL Gateway and its devices with the Secure Access Concentrator Remote Server.
Alarm ID	The Product ID (also called Alarm ID) for the SAL Gateway. This ID should start with a 5 and include ten digits. The system uses the value in the this field to uniquely identify the source of Gateway alarms in the Secure Access Concentrator Core Server.

Name	Description
Alarm Enabled	Enables the alarming component of the SAL Gateway. This check box must be selected for the SAL Gateway to send alarms.
Inventory Collection	Enables inventory collection for the SAL Gateway. When this check box is selected, SAL Gateway collects inventory information about the supported managed devices and sends it to the Secure Access Concentrator Core Server for Avaya reference. This feature is intended for services personnel working on tickets and must review the configuration of managed devices. For more information on this feature, see the *Secure Access Link Gateway 1.8 Implementation Guide*. This document is available at http://support.avaya.com
Inventory collection schedule	Interval in hours at which the SAL Gateway collects inventory data.

Related topics:

Registering the system on page 36

Configuring a proxy server

About this task

Use the Proxy Server page to configure proxy settings if required for SAL Gateway to communicate with the Secure Access Concentrator Remote Server and the Secure Access Concentrator Core Server.

Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Proxy**.
2. On the Proxy Server page, complete the following fields:
   - **Use Proxy**
   - **Proxy Type**
   - **Host**
   - **Port**
3. Click **Apply**.

4. (Optional) Once you complete configuration of SAL Gateway, you can use the **Test** button to test connectivity to the proxy server.

   See the *Secure Access Link Gateway 2.2 Implementation Guide* for more information. This document is available at http://support.avaya.com.

Next steps

After completing configuration of SAL Gateway, you must apply configuration changes for the configuration to take effect. This task is performed on the Apply Configuration Changes page and restarts the SAL Gateway. To minimize disruption of services and alarms, apply configuration changes only after you finish configuration of SAL Gateway.

Related topics:

Proxy Server field descriptions on page 75

Applying configuration changes on page 81

Proxy Server field descriptions

The Proxy Server page of the SALGateway user interface provides you the options to view and update the proxy server configuration for SAL Gateway. SAL Gateway uses the proxy configured on this page to establish external connections.

The page displays the following fields:

Name	Description
Use Proxy	Check box to enable the use of a proxy server.
Proxy Type	The type of proxy server that is used. Options are: • **SOCKS 5** • **HTTP**
Host	The IP address or the host name of the proxy server. SAL Gateway takes both IPv4 and IPv6 addresses as input.
Port	The port number of the Proxy server.
Login	Login if authentication is required for the HTTP proxy server. **Important:** SAL Gateway in System Platform does not support authenticating proxy servers.
Password	Password for login if authentication is required for the HTTP proxy server.

Name	Description
	Important: SAL Gateway in System Platform does not support authenticating proxy servers.
Test URL	The HTTP URL used to test the SAL Gateway connectivity through the proxy server. The Gateway uses the proxy server to connect to the URL you provide.

The page displays the following buttons:

Name	Description
Test	Initiates a test of the SAL Gateway connectivity through the proxy server to the URL specified in the **Test URL** field. You can initiate a test before or after applying the configuration changes.
Edit	Makes the fields on the Proxy Server page available for editing.
Apply	Saves the configuration changes.

Configuring SAL Gateway communication with a Concentrator Core Server

About this task

Use the Core Server page of the SAL Gateway user interface to review settings for communication between SAL Gateway and a Secure Access Concentrator Core Server (SACCS) at Avaya Data Center. The SACCS handles alarming and inventory. Do not change the default settings unless you are explicitly instructed to do so.

Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Core Server**.
   The Core Server page is displayed.
2. Do not change the default settings on this page.

   See the *Secure Access Link Gateway 2.2 Implementation Guide* for more information. This document is available at http://support.avaya.com.
3. (Optional) Once you complete configuration of SAL Gateway, you can use the **Test** button to test connectivity to the defined Secure Access Concentrator Core Servers.

See the *Secure Access Link Gateway 2.2 Implementation Guide* for more information. This document is available at http://support.avaya.com.

Next steps

After completing configuration of SAL Gateway, you must apply configuration changes for the configuration to take effect. This task is performed on the Apply Configuration Changes page and restarts the SAL Gateway. To minimize disruption of services and alarms, apply configuration changes only after you finish configuration of SAL Gateway.

The system does not connect to the new Secure Access Concentrator Core Server until you restart the SAL Gateway.

Related topics:

Core Server field descriptions on page 77

Applying configuration changes on page 81

Core Server field descriptions

Name	Description
Passphrase	Default passphrase is `Enterprise-production`. Do not change the default unless you are explicitly instructed to do so. This passphrase is used to establish a channel for communication between the SAL Gateway and the Secure Access Concentrator Core Server.
Primary Core Server	IP Address or the host name of the primary Secure Access Concentrator Core Server. The default value is `secure.alarming.avaya.com`.
Port	Port number of the primary Secure Access Concentrator Core Server. The default value is `443`.
Secondary Core Server	This value must match the value in the **Primary Core Server** field.
Port	This value must match the value in the **Port** field for the primary server.

Configuring SAL Gateway communication with a Concentrator Remote Server

About this task

Use the Remote Server page of the SAL Gateway user interface to review settings for communication between SAL Gateway and a Secure Access Concentrator Remote Server

(SACRS) at Avaya Data Center. The SACRS handles remote access, and updates models and configuration. Do not change the default settings unless you are explicitly instructed to do so.

Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Remote Server**.
   The Remote Server page appears.
2. Do not change the default settings on this page unless you are explicitly instructed to do so.
3. (Optional) Once you complete configuration of SAL Gateway, you can use the **Test** button to test connectivity to the defined Secure Access Concentrator Remote Servers.

   See the *Secure Access Link Gateway 2.2 Implementation Guide* for more information. This document is available at http://support.avaya.com.

Next steps

After completing configuration of SAL Gateway, you must apply configuration changes for the configuration to take effect. This task is performed on the Apply Configuration Changes page and restarts the SAL Gateway. To minimize disruption of services and alarms, apply configuration changes only after you finish configuration of SAL Gateway.

The system does not connect to the new Secure Access Concentrator Remote Servers until you restart the SAL Gateway.

When you restart the SAL Gateway, the system terminates all active connections.

Related topics:

Remote Server field descriptions on page 78

Applying configuration changes on page 81

Remote Server field descriptions

Name	Description
Primary Remote Server	The IP address or host name of the primary Secure Access Concentrator Remote Server. The default value is `sl1.sal.avaya.com`.
Port	The port number of the primary Secure Access Concentrator Remote Server. The default value is `443`.
Secondary Remote Server	This value must match the value in the **Primary Remote Server** field.

Name	Description
Port	This value must match the value in the **Port** field for the primary server.

Configuring NMS

About this task

Use this procedure to specify SNMP trap destinations. When you configure Network Management Systems (NMSs), the SAL Gateway copies traps and alarms (encapsulated in traps) to each NMS that you configure.

Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **NMS**.
2. On the Network Management Systems page, complete the following fields:
   - **NMS Host Name/ IP Address**
   - **Trap port**
   - **Community**
3. Click **Apply**.
4. (Optional) Use the **Add** button to add multiple NMSs.

   See the *Secure Access Link Gateway 2.2 Implementation Guide* for more information. This document is available at http://support.avaya.com.

Next steps

After completing configuration of SAL Gateway, you must apply configuration changes for the configuration to take effect. This task is performed on the Apply Configuration Changes page and restarts the SAL Gateway. To minimize disruption of services and alarms, apply configuration changes only after you finish configuration of SAL Gateway.

Related topics:

Network Management Systems field descriptions on page 79

Applying configuration changes on page 81

Network Management Systems field descriptions

Name	Description
NMS Host Name/ IP Address	The IP address or host name of the NMS server.
Trap port	The port number of the NMS server.

Name	Description
Community	The community string of the NMS server. Use `public` as the **Community**, as SAL agents support only public as community at present.

Managing service control and status

About this task

Use this procedure to view the status of a service, stop a service, or test a service that the SAL Gateway manages.

Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Service Control & Status**.
   The system displays the Gateway Service Control page. The page lists the following services:
   - **SAL Agent**
   - **Alarming**
   - **Inventory**
   - **Health Monitor**
   - **Remote Access**
   - **SAL Watchdog**
   - **SAL SNMP Sub-agent**
   - **Package Distribution**
   - **SAL Agent Watchdog**

   The Gateway Service Control page also displays the status of each service as:
   - **Stopped**
   - **Running**
2. Click one of the following buttons:
   - **Stop** to stop a service.
   - **Start** to start a service that is stopped.
   - **Test** to send a test alarm to the Secure Access Concentrator Core Server.

Important:

Use caution if stopping the Remote Access service. Doing so will block you from accessing SAL Gateway remotely.

Applying configuration changes

Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Apply Configuration Changes**.
   The system displays the Apply Configuration Changes page.
2. Click the **Apply** next to **Configuration Changes**.

   See the *Secure Access Link Gateway 2.2 Implementation Guide* for more information. This document is available at http://support.avaya.com.

   When you click **Apply**, the system restarts the SAL Gateway and updates the Gateway with the new values you configured.

   The SAL Gateway misses any alarms that are sent while it restarts.

Managed element worksheet for SAL Gateway

Use this worksheet to record the information required by an administrator to add managed devices to the SAL Gateway.

System Domain (Domain-0) does not have alarming enabled; however, it has its own Product ID (Alarm ID).

Console Domain (cdom or udom) has alarming enabled. System Domain sends all syslog (system logs) to Console Domain, which then triggers alarms on behalf of System Domain.

Important:

For High Availability Failover configurations, you must have two different solution element IDs (SEIDs) for System Domain (Domain-0): one for the active System Domain and one for the standby System Domain. You must administer both SEIDs in the SAL Gateway user interface.

Managed device (virtual machine)	IP Address	SE ID	Product ID	Model	Notes
System Domain (Domain-0)				VSP_2.0.0.0	
Console Domain (cdom or udom)				VSPU_2.1.1.2	

Related topics:

Adding a managed element on page 82

Adding a managed element

Before you begin

Complete the Managed Element Worksheet for SAL Gateway.

About this task

Perform this procedure for each Solution Element ID (SE ID) that is provided in the registration information from Avaya.

Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Secure Access Link Gateway** > **Managed Element**.
2. On the Managed Element page, click **Add new**.
3. Complete the fields on the page as appropriate.
4. Click **Add**.
5. Click **Apply** to apply the changes.

Next steps

After completing configuration of SAL Gateway, you must apply configuration changes for the configuration to take effect. This task is performed on the Apply Configuration Changes page and restarts the SAL Gateway. To minimize disruption of services and alarms, apply configuration changes only after you finish configuration of SAL Gateway.

Related topics:

Applying configuration changes on page 81
Managed element worksheet for SAL Gateway on page 81
Managed Element field descriptions on page 83

Managed Element field descriptions

Name	Description
Host Name	Host name for the managed device. This must match the host name on the Network Configuration page of the System Platform Web Console (**Server Management** > **Network Configuration** in the navigation pane).
IP Address	IP address of the managed device.
NIU	Not applicable for applications that are installed on System Platform. Leave this field clear (not selected).
Model	The model that is applicable for the managed device.
Solution Element ID	The Solution Element ID (SE ID) of the device. The SE ID makes it possible for Avaya Services or Avaya Partners to connect to the managed applications remotely.
Product ID	The Product ID (also called Alarm ID). The Product ID is included in alarms that are sent to alarm receivers from the managed device. The Product ID identifies the device that generated the alarm.
Provide Remote Access to this device	Check box to allow remote connectivity to the managed device.
Transport alarms from this device	(Optional) Check box to enable alarms from this device to be sent to the Secure Access Concentrator Core Server.
Collect Inventory for this device	Check box to enable inventory collection for the managed device. When this check box is selected, SAL Gateway collects inventory information about the managed device and sends it to the Secure Access Concentrator Core Server for Avaya reference. This feature is intended for

Name	Description
	services personnel working on tickets and must review the configuration of managed devices. For more information on this feature, see the *Secure Access Link Gateway 1.8 Implementation Guide*. This document is available at http://support.avaya.com.
Inventory collection schedule	Interval in hours at which the SAL Gateway collects inventory information about the managed device.
Monitor health for this device	Check box to enable health monitoring of the managed device by SAL Gateway. SAL Gateway uses heartbeats to monitor health. Heartbeats must be configured on the device.
Generate Health Status missed alarm every	Interval in minutes at which SAL Gateway generates an alarm if it does not receive a heartbeat from the managed device. You must restart the SAL Gateway for the configuration changes to take effect. SAL Gateway starts monitoring heartbeats from the device after the restart and generates alarms if it does not receive a heartbeat within the configured interval.
Suspend health monitoring for this device	Check box to suspend health monitoring for the managed device.
Suspend for	Number of minutes to suspend health monitoring for the managed device. SAL Gateway resumes monitoring the device after the configured time elapses.

Using a stand-alone SAL Gateway

Adding an SNMP trap receiver

About this task

Use this procedure to add an SNMP trap receiver for System Platform. If you are using a stand-alone SAL Gateway, you must add it as an SNMP trap receiver.

Procedure

1. In the navigation pane of the System Platform Web Console, click **Server Management** > **SNMP Trap Receiver Configuration**.

2. On the SNMP Trap Receiver Configuration page, complete the following fields:
    - **IP Address**
    - **Port**
    - **Community**
3. Click **Add SNMP Trap Receiver**.

Disabling SAL Gateway

The locally embedded SAL must be in a disabled state if your Avaya Aura® solution requires a stand-alone SAL Gateway server.

Disable the local SAL if your Avaya Aura® solution requires a higher-capacity, stand-alone SAL Gateway server. This configuration is more appropriate for handling SNMP trap/alarm forwarding and Avaya remote services for a larger Enterprise solution.

Disable the SAL Gateway running on the Services Virtual Machine if you determine, for example, that after expanding your existing Avaya Aura® solution, this SAL Gateway no longer has enough capacity to handle the increased requirements for trap/alarm forwarding and remote services. In this case, install and configure the SAL Gateway on an independent server elsewhere in your network.

About this task

Use this procedure to disable the SAL Gateway running on the System Platform Services Virtual Machine.

Note:

- If you installed System Platform version 6.2 or later, and deselected the **Enable Services VM** default setting during that process, then neither the embedded SAL nor the local Services Virtual Machine will be active. (With System Platform version 6.2 or later, SAL no longer runs on the Cdom virtual machine, but instead runs on a Services Virtual Machine or services_vm.) In this scenario, you take no action to disable the embedded SAL Gateway before installing and launching the SAL Gateway on a stand-alone server.
- With System Platform version 6.2 or later, disabling the Services Virtual Machine also disables the local SAL gateway running on that virtual machine.

Procedure

1. In the navigation pane of the System Platform Web Console , click **Server Management** > **SAL Gateway Management**.
2. On the SAL Gateway Management page, click **Disable SAL Gateway**.

Installing a solution template

Before you begin

- Determine if you will be using an Electronic Pre-installation Worksheet (EPW) file to configure the solution template while installing it. You must create the EPW file before installing the template.
- Ensure that your browser option to block pop-up windows is disabled.

About this task

Important:

If you have a System Platform High Availability configuration, do not install a template on the standby node. If you do, you will be unable to start High Availability operation. If you are using a bundled System Platform installation (with a solution template), disable the template installation on the standby server. The solution template is propagated from the active node to the standby node when you start High Availability operation.

Important:

Some Avaya Aura® solutions do not support template installation using all four of the possible file source options (PLDS, CD/DVD, USB, SP_Server). Refer to template installation topics in your Avaya Aura® solution documentation to determine the correct option for installation of your solution template.

Approximate installation time for System Manager is 15 minutes.

Procedure

1. Log in to the System Platform Web Console as admin.
2. If installing from a USB flash drive, connect the flash drive to the server.
3. If installing from a single CD or DVD, insert the CD or DVD in the server CD or DVD drive.
4. If installing from multiple DVDs, copy the DVDs to the server:
   a. Click **Server Management** > **File Manager** in the navigation pane.
   b. Insert the first DVD.
   c. Click **View DVD/CD**.
   d. After the system mounts and reads the DVD, click **Copy Files**.
   The files are copied to the /vsp-template/cdrom directory on the server.
   e. When the system finishes copying the files, insert the second DVD.
   f. Click **View DVD/CD**.
   g. After the system mounts and reads the DVD, click **Copy Files**.
   The files are copied to the /vsp-template/cdrom directory on the server.
   h. Repeat for remaining DVDs

i. After the system finishes copying the files, select the template in the **/vsp-template/** field of the **Copy from Server DVD/CD** area.

j. Click **Finalize copy**.
The files are copied to the template-specific directory that you selected in the previous step, and the cdrom directory is deleted.

> ❗ **Important:**
>
> If the writable DVD does not mount, write the ISO images to high quality DVDs and use a slower write speed.

5. Click **Virtual Machine Management** > **Templates** in the navigation pane.

   The system displays the Search Local and Remote Template page. Use this page to select the template to install on System Platform.

6. Click **Upgrade** next to the virtual machine that you want to upgrade, and then, in the **Install Template From** field, select the location of the software to be installed.

   If you copied multiple DVDs to the server, select **SP Server**.

   > ✱ **Note:**
   >
   > If the software is located on a different server (for example, Avaya PLDS or HTTP), and depending on your specific network environment, configure a proxy if necessary to access the software. See Configuring a proxy.

7. If you selected **HTTP** or **SP Server** in the **Install Template From** field, enter the complete URL or path of the template files.

8. Click **Search** to display a list of template descriptor files (each available template has one template descriptor file).

9. On the Select Template page, click the required template, and then click **Select** to continue.
   The system displays the Template Details page with information on the selected template and its Virtual Appliances.

10. Click **Install** to start the template installation.

    > ✱ **Note:**
    >
    > System Platform automatically performs a hardware check of the server platform at this time. Servers supported by Avaya must meet all prerequisites for the System Platform, any platform options, and a specific solution template. If the server hardware check performed at this time passes, template installation proceeds normally. However, in a circumstance where the hardware check halts template installation, one or both of the following messages appear:
    >
    > - Template Future Upgrade warning – `There is enough disk space to proceed with the current template installation/upgrade.`

`However, there might not be enough disk space for a future template upgrade.`

- Insufficient disk space or memory resources message – `Insufficient resources to install this template (<template_name>).`

In either case, capture the exact details of the error message and go to the Avaya Support website at http://support.avaya.com/ for current documentation, product notices, knowledge articles related to the topic, or to open a service request.

If the template you selected supports an Electronic Pre-installation Worksheet (EPW), the system prompts you to continue without an EPW or to provide an EPW file. The system also prompts you with pages that require your input such as IP addresses for the applications that are included in the template. These pages vary according to the template you are installing. If you provided an EPW file, some of these pages typically contain data from the EPW.

Important:

If you are installing from a USB flash drive, remove the flash drive when the installation is complete. The presence of a flash drive connected to the server could prevent that server from rebooting.

Search Local and Remote Template field descriptions

Use the Search Local and Remote Template page to select the template to install on System Platform, to upgrade an installed template, or to delete an installed template.

Name	Description
Install Template From	Locations from which you can select a template and install it on System Platform. Available options are as follows: **Avaya Downloads (PLDS)** The template files are located in the Avaya Product Licensing and Delivery System (PLDS) Web site. You must enter an Avaya SSO login and password. The list will contain all the templates to which your company is entitled. Each line in the list begins with the “sold-to” number to allow you to select the appropriate template for the site where you are installing. Hold the mouse pointer over the selection to view more information about the “sold-to” number. **HTTP** The template files are located on an HTTP server. You must enter the template URL information.

Name	Description
	SP Server The template files are located in the `/vsp-template` file system in the Console Domain of the System Platform server. **SP CD/DVD** The template files are located on a CD or DVD in the CD/DVD drive on the server. **SP USB Disk** The template files are located on a USB flash drive connected to the server.
SSO Login	Active only when you select the **Avaya Downloads (PLDS)** option to search for a template. Login id for logging on to Single Sign On.
SSO Password	Active only when you select the **Avaya Downloads (PLDS)** option to search for a template. Password for Single Sign On.

Search Local and Remote Template button descriptions

Name	Description
Install	Installs the solution template. This button is displayed only if no template is currently installed on System Platform.
Configure Proxy	Active only when you select the HTTP option to search for a solution template. Lets you configure a proxy for the HTTP address. If necessary, configure a proxy for Secure Access Link (SAL) and alarming functions to access the internet.
Upgrade	Upgrades the installed solution template from the selected template location option. This button is displayed only if a template is installed on System Platform.
Delete	Deletes the currently installed and active template. This button is displayed only if a template is installed on System Platform.

Configuring System Platform High Availability

About System Platform High Availability

System Platform High Availability is an optional feature that provides different levels of services continuity. This feature is available with some, but not all, Avaya Aura® solution templates. For example, the Communication Manager template does not currently use the System Platform High Availability feature.

For more details about System Platform High Availability, refer to administration topics relevant to this functionality in your Avaya Aura® solution documentation.

Template administration during High Availability operation

System Platform does not support installation, upgrade, or deletion of templates while running the system in an active High Availability mode. The web console displays a warning message on template pages, and you cannot perform any actions associated with them.

To install, upgrade, or delete a template, you must first stop High Availability and remove its configuration. Templates must be installed, upgraded, or deleted only on the preferred node in a High Availability configuration.

You must perform all template operations while logged on to the preferred node. Once you finish template configuration, you can restart High Availability operation in the desired mode

Important:

If you have a System Platform High Availability configuration, do not install a template on the standby node. If you do, you will be unable to start High Availability operation. If you are using a bundled System Platform installation (with a solution template), disable the template installation on the standby server. The solution template is propagated from the active node to the standby node when you start High Availability operation.

Prerequisites for High Availability configuration

Introduction to High Availability prerequisites

For Avaya Aura® solutions that support System Platform High Availability operation, configuration prerequisites exist in two areas:

- Common prerequisites for all System Platform High Availability configurations
- Prerequisites for a specific type of System Platform High Availability (for example, locally redundant HA)

System Platform supports Locally Redundant High Availability configurations

You must satisfy all of the Common and HA-specific prerequisites before attempting to configure System Platform High Availability.

Note also that some solution templates support alternatives to System Platform High Availability. To determine specific support for either System Platform High Availability or an alternative template-driven implementation of solution High Availability, refer to feature support information in your Avaya Aura® solution documentation.

Common prerequisites for all High Availability modes

If your Avaya Aura® solution template supports any mode of System Platform High Availability operation, you must satisfy all applicable prerequisites identified in this topic.

Servers

- Two servers with the same hardware configuration. At a minimum, the servers must have identical memory, number of processors, total disk space or free disk space as determined by template requirements.
- The servers must have a spare Gigabit network interface to be dedicated exclusively to System Platform High Availability services. The servers must be connected on the same ports on both machines.
- Verify that System Platform and the solution template both support the specific server.

Cabling

The System Platform High Availability physical configuration requires an Ethernet CAT5E cable with straight-through wiring for the connection from local server port eth0 to a port on the local default gateway router. This provides each server with connectivity to the public IP network. This connection also carries Ping traffic between each server and the default gateway router.

Software

- Verify that the same version of System Platform, including software patch updates, have been installed on the primary and secondary servers.

  Note:

  For Avaya Aura solutions deployed in a System Platform High Availability configuration, you must install/apply patches on both the primary and secondary servers independently. The primary server does not automatically replicate System Platform patches to the secondary server.

- Record the cdom username and password for logon to the primary and secondary System Platform servers when necessary.
- If you have a System Platform High Availability configuration, do not install a template on the standby node. If you do, you will be unable to start High Availability operation. If you are using a bundled System Platform installation (with a solution template), disable the template installation on the standby server. The solution template is propagated from the active node to the standby node when you start High Availability operation.

Prerequisites for locally redundant High Availability

If your Avaya Aura® solution template will be using System Platform FRHA, and/or MPHA with LMHA High Availability modes, you must satisfy all of the common prerequisites for all HA modes, plus the prerequisites specifically for Locally Redundant High Availability described in this topic.

Network Interface Cards (NICs)

- Both servers should have a spare network interface dedicated exclusively to High Availability data replication, as follows:
  - FRHA: 1 Gb/s interface
  - MPHA and LMHA: 10 Gb/s interface

Cabling

- Both servers must be in close proximity for interconnection by means of a high-speed Ethernet cable with crossover signal wiring. This cable carries data replication traffic between the primary and secondary servers. It also carries heartbeat messaging between the two servers.

  Note:

  The Ethernet specification limit for the length of this cable between the primary and secondary servers is 100 meters. This interconnection must not include a layer-2 switch. The same Ethernet port on each server must be used to create the crossover connection, for example, eth2 to eth2, eth3 to eth3, or eth4 to eth4. The minimum acceptable cable type for this node-to-node crossover connection is Ethernet CAT5E. For installation sites with higher than normal electrical or signal noise in some areas, use Ethernet type CAT5A cabling for the crossover connection. Type CAT6A cable provides the best levels of shielding against crosstalk and external signal interference.

- For FRHA operation, use a type CAT5E Ethernet cable *with cross-over wiring* for the high-speed crossover connection between a 1Gb/sec NIC port on the primary server to a 1 Gb/sec NIC port on the secondary server. You must use the same port on both servers, typically eth 2 to eth2. If eth2 is unavailable, you cannot use eth 0 or eth1 for the crossover connection, but you can use other available 1Gb/s Ethernet ports on the two servers.
- For MPHA (and implicitly LMHA operation for standard Cdom and Services virtual machines), use a type CAT6A Ethernet 10 Gb/sec cable *with cross-over wiring* for the high-speed crossover connection between a 10Gb/sec NIC port on the primary server to a 10 Gb/sec NIC port on the secondary server. You must use the same port on both servers, typically eth 2 to eth2. If eth2 is unavailable, you cannot use eth 0 or eth1 for the crossover connection, but use other available 10 Gb/s Ethernet ports on the two servers.

Networking for locally redundant High Availability

- Install both servers on the same IP subnetwork.
- Document IP addresses for the following Ping targets:
  - The IP address of the default gateway router interface local to the primary (preferred) server. (The primary server requires this target to assure connectivity to the public network.)

  - The IP address of the default gateway router interface local to the standby server. (The standby server requires this target to assure connectivity to the public network.)
  - The IP address of any servers (not including System Platform servers) deployed as part of your Avaya Aura® solution. Add these servers as optional Ping targets, to help extend connectivity monitoring (using Ping) throughout the solution topology. Refer to the requirements of your specific solution template.

- Ensure that the default gateway replies to ICMP pings from each of the System Platform nodes. Use each server's command line to check:

  `ping <default_gateway_IP_address>`.

  Verify the ping responses to each server from the default gateway, each containing a ping response time.

Configuring System Platform High Availability

Configuring locally redundant High Availability

Before you begin

You must have a user role of Advanced Administrator to perform this task.

You must complete:

- Common prerequisites for all System Platform High Availability configurations
- Prerequisites for a specific type of System Platform High Availability (for example, locally redundant HA)

About this task

- Perform this task only on the System Platform server chosen to be the Preferred (primary) Node in the High Availability pair.
- The primary server propagates its configuration to the secondary (standby) server when you start High Availability operation.
- This procedure synchronizes all required configuration settings from the preferred node to the standby node so that the standby node can assume the role of active node if required.
- If you have a System Platform High Availability configuration, do not install a template on the standby node. If you do, you will be unable to start High Availability operation. If you are using a bundled System Platform installation (with a solution template), disable the template installation on the standby server. The solution template is propagated from the active node to the standby node when you start High Availability operation.
- During disk synchronization (typically while HA operations are starting up) the High Availability software automatically adjusts the default rate of disk synchronization (typically 100 MB/sec) to the speed of the crossover interface between the two nodes.
- After starting HA, you can log on to the Web Console of the active server.

Procedure

1. Log in to the Web Console of the server chosen to be the preferred node.

   Use the IP address of the server's Cdom virtual machine when logging on to the Web Console.

2. Click **Server Management** > **High Availability**.

   The High Availability page displays the current status of the High Availability configuration.

3. Click **Configure HA**.

   Note:

   The **Configure HA** button in the Web Console will be disabled whenever the server has no physical or logical interfaces available for High Availability configuration.

4. On the Configure HA page, enter the appropriate information to configure High Availability operation for all template virtual machines.

   If your Avaya Aura® solution template supports any enhanced System Platform High Availability modes in addition to the default (Fast Reboot High Availability, or FRHA), you can change the mode of High Availability protection on template virtual machines. To verify solution support for any System Platform enhanced High Availability modes, refer to your solution documentation. The Web Console displays different HA configuration fields, according to the HA modes supported by your solution template.

5. Click **Create**.

6. After the system finishes creating the High Availability configuration, click **Start HA** and confirm the displayed warning.

   The Start HA button is visible only if High Availability is fully configured but inactive.

7. Click **Server Management** > **High Availability**.

   You can check the status of virtual machines on the High Availability page and ensure that the data replication software is synchronizing virtual machine disk volumes on the active and standby servers.

   For virtual machines configured for Fast Reboot High Availability (FRHA), the HA virtual machine status on the High Availability page should display `Connected and Synching` first and then `Running` when the logical disk volumes on the active and standby servers achieve synchronization.

   For virtual machines supporting for Machine Preserving High Availability (MPHA), the HA virtual machine status on the High Availability page should display `Ready for Interchange` when both disk and memory on the active and standby servers achieve synchronization.

High Availability field descriptions

This initial System Platform High Availability page contains mainly read-only fields associated with the current status of the High Availability software, as well as its primary and secondary server nodes. The page otherwise includes a single button, **Configure HA**.

Button	Description
Configure HA	Invokes the Configure HA page to begin the process of configuring or modifying the configuration of System Platform High Availability **Note:** The **Configure HA** button is disabled whenever the server has no physical or logical interfaces available for High Availability configuration.

Configure HA field descriptions

The following tables describe:

- The status of individual virtual machines that are running on the primary server in a System Platform server.
- Fields for configuring System Platform local High Availability operation.
- Buttons to aid you in navigating through High Availability configuration, creating (applying) a High Availability configuration on primary and secondary servers, starting High Availability, manually interchanging High Availability server roles, stopping High Availability, and removing High Availability when needed.

Virtual Machine Protection Mode configuration

VM Name	VM Description	Protection Mode
`cdom`	System Platform Console Domain	The mode of System Platform High Availability (SPHA) protection configured on the cdom virtual machine: Fast Reboot (FRHA) If Machine Preserving High Availability (MPHA) is selected for the solution template, the protection mode for all other virtual machines automatically changes to Live Migration.
`services_vm`	System Platform Services Domain	The mode of System Platform High Availability (SPHA) protection configured on the

VM Name	VM Description	Protection Mode
		services_vm virtual machine: Fast Reboot (FRHA) If Machine Preserving High Availability (MPHA) is selected for the solution template, the protection mode for all other virtual machines automatically changes to Live Migration.
<solution_template_vm>	Avaya Aura® solution template	The mode of System Platform High Availability (SPHA) protection configured on a solution template virtual machine. If the VM supports multiple SPHA protection modes, a drop-down menu is available for selecting alternate modes: • Fast Reboot (FRHA) • Machine Preserving (MPHA) If Machine Preserving High Availability (MPHA) is selected for the solution template, the protection mode for all other virtual machines automatically changes to Live Migration.

Local and remote server Cdom and Dom0 network interface configuration

Name	Description
Local Server (Dom-0) IP Name	Host name of the Domain-0 VM on the preferred active server.
Local Server (Dom-0) IP Address	IP address of the Domain-0 VM on the preferred active server.
Remote cdom IP address	IP Address of the Console Domain VM on the standby node.
Remote cdom user name	User name for accessing the Console Domain VM on the standby node.
Remote cdom password	Password for accessing the Console Domain VM on the standby node.

Name	Description
Crossover network interface	Network interface connected to the standby server. Required for inter-node communication supporting node arbitration, High Availability failover, and High Availability switchover events.

Ping targets configuration

Name	Description
Ping Target (IP Address/HostName)	IP address or host name of the gateway to the network. You can add multiple ping targets to verify if the System Platform server is connected to network.
Interval (sec)	Interval after which the local System Platform server sends ICMP pings to listed ping targets.
Timeout (sec)	Timeout interval after which no ICMP reply indicates a network failure.

Buttons

Name	Description
Create	Applies to the primary and secondary nodes in the High Availability configuration entered on the Configure HA page. When the system completes this operation, you can click **Start HA**.
Start HA	Starts the System Platform High Availability configuration applied to the primary and secondary nodes when you clicked **Create**. Also restarts a previously running High Availability configuration after you clicked **Stop HA** to perform certain HA-related administrative tasks.
Stop HA	Stops System Platform High Availability on the primary and secondary nodes. Does not remove the High Availability configuration.
Remove HA	Removes the System Platform High Availability configuration from the primary or secondary nodes.
Add Ping Target	Adds a new ping target.
Edit	Allows you to edit any existing ping target you select in the adjacent check box.

Name	Description
Delete	Allows you to delete any existing ping target you select in the adjacent check box.
Manual Interchange	Manually triggers a graceful switch-over of the current active and standby nodes in the System Platform High Availability configuration.

High Availability start/stop

High Availability start

You can **Start HA** (start High Availability) operation after committing the feature to the active node configuration. The active node will propagate this configuration to the standby node at commit time. When you start High Availability operation, the console domain and template virtual machines restart on the active and standby nodes.

Important:

If you have a System Platform High Availability configuration, do not install a template on the standby node. If you do, you will be unable to start High Availability operation. If you are using a bundled System Platform installation (with a solution template), disable the template installation on the standby server. The solution template is propagated from the active node to the standby node when you start High Availability operation.

High Availability stop

Stopping High Availability operation (using the **Stop HA** button) returns System Platform to standard operation without High Availability protection. (This action does not remove the High Availability configuration from either node.)

Important:

Stopping High Availability operations during disk synchronization could corrupt the file system of the standby console domain. Check the status of virtual machine disk synchronization on the High Availability page of the web console.

Once High Availability operations halt:

- the two nodes function independently in simplex mode.
- the system no longer propagates VM disk changes (FRHA, LMHA) or VM CPU memory changes (MPHA) from the active node to the standby node.
- you can access the Web Console on the standby server by using its IP address (provided during configuration of the High Availability feature).

Related topics:

Starting System Platform High Availability on page 99
Stopping System Platform High Availability on page 99

Starting System Platform High Availability

This procedure synchronizes all required configuration settings from the preferred node to the standby node so that the standby node can assume the role of active node if required.

About this task

Whether you have completed a new System Platform installation or a System Platform upgrade, your Avaya Aura solution documentation should indicate which of the two High Availability servers will be the preferred node. You must **Start HA** from that node.

Important:

If you are performing a platform upgrade, do not start High Availability operation until after you commit the platform upgrade on both the primary and secondary servers.

Note:

- If you are restarting Fast Reboot High Availability (FRHA) operation after performing **Stop HA**, you can restart anytime after FRHA halts.
- If you are restarting Machine Preserving (and implicitly, Live Migration) High Availability (MPHA/LMHA) after performing **Stop HA**, you can restart anytime after MPHA/LMHA halts.

Note:

When starting HA, System Platform removes all bonded interfaces defined earlier on the standby node, but then automatically propagates (duplicates) all bonded interfaces defined on the active node to the standby node. This operation assures that both nodes have the same bonded interface configuration after HA startup.

Procedure

1. Click **Server Management** > **High Availability**.
2. Click **Start HA** and confirm the displayed warning.
3. Click **Server Management** > **High Availability**.

   Verify the progress of virtual machine replication on the High Availability page.

Stopping System Platform High Availability

Before you begin

Important:

Stopping High Availability operations during disk synchronization could corrupt the file system of the standby console domain. Check the status of virtual machine replication on the High Availability page of the Web Console.

About this task

This procedure stops Fast Reboot High Availability (FRHA) operation but does not remove its configuration from System Platform. You can restart FRHA operation anytime after performing this procedure.

The same is true for Machine Preserving and Live Migration high availability modes of operation (MPHA/LMHA).

Procedure

1. Click **Server Management** > **High Availability**.
2. Click **Stop HA** and confirm the displayed warning.

   Verify the status of virtual machine replication on the High Availability page.

Manually switching High Availability server roles

Before you begin

- All virtual machine disks on the active and standby nodes must be in a synchronized state (contain the same data). Check the **Disk Status** area of the High Availability page.
- MPHA-protected virtual machine memory on the active and standby nodes must be in a synchronized state (contain the same data). Check the **Disk Status** and **Memory Status** areas of the High Availability page.

About this task

Use this procedure for a variety of administrative, maintenance, or troubleshooting tasks affecting only one server. For example, use this procedure prior to replacing a hardware module on the active node in an Avaya Aura® system enabled with High Availability protection.

Procedure

1. From the **Server Management** menu, click **High Availability**.
2. Click **Manual Interchange** on the High Availability page.
3. Click **OK** to confirm the warning message.

Removing the High Availability configuration

Use this procedure to permanently remove the High Availability configuration.

Before you begin

- You have stopped System Platform High Availability.

About this task

Use this procedure, for example:

- to remove the HA configuration from Avaya Aura® solution servers prior to a System Platform upgrade. Removing the HA configuration from the primary/active HA server also removes the HA configuration from the standby server automatically.
- to restore Avaya Aura® solution servers in an HA configuration to simplex operation

Procedure

1. Log on to the Web Console for the primary/active HA server.
2. Click **Server Management > High Availability**.
3. Click **Remove HA** and confirm the displayed warning.

Installing System Manager

Downloading System Manager from PLDS

Procedure

1. To gain access to the Avaya Product Licensing and Delivery System (PLDS) website, in the Web browser, type `http://plds.avaya.com`.
2. Click **Log in with my password**.
3. Enter the login ID and the password.

   Note:

   Your login ID is your email address.
4. Click **Log In**.
5. On the Home page, expand **Asset Mgmt** and click **View Downloads**.
6. On the Downloads page, in the **%Company** field, enter the company name.
7. In the **Application** field, click `System Manager`.
8. Click **Search Downloads**.

9. From the Software Downloads list, download the following files to the `/tmp` directory on your computer:
    - The `System_Manager_06_03.iso` file. The ISO file contains the following files:
        - `pre-install.war` (war file)
        - `System_Manager_06_03.tar` (tar file)
        - `System_Manager_06_03_Post_Deploy.tar` (tar file)
        - `SystemManager.mf` (mf file)
        - `SystemManager.ovf` (ovf file)

      You can also download these files individually from the PLDS website.
    - The `System_Manager_R6.3_FP2_S4_1399.bin` file
10. On the About the Download Manager page, click **Click to download your file now**.
11. If the system displays an error message regarding ActiveX installation, then install ActiveX and continue the download.
12. When the system displays a security warning, click **Install**.

    When the installation is complete, the Web page on PLDS displays the downloads again with a checkmark.

Installation methods

Use one of the following methods to install the System Manager template:

- Download and copy the ISO file to System Platform Console and install the template.
- Burn the ISO image to a DVD and install the template using the DVD.

Related topics:

Installing the System Manager 6.3 template using ISO on page 102
Installing System Manager using a DVD on page 107

Installing the System Manager 6.3 template using ISO

When you install System Manager on a virtual machine using the System Manager template, the system installs the Linux (CentOS) operating system along with the System Manager software.

Before you begin

- Disable the pop-up blocker for the Web browser to proceed with the installation.
- Download the System_Manager_06_03..iso file that contains the System Manager installation files.

Procedure

1. Perform the following procedures:
   a. Using ssh, log in to System Platform on C-dom as `root`.
   b. At the command prompt, type `mkdir /iso`.
   c. Copy the System_Manager_06_03..iso file to the `/tmp` folder using the application such as WinSCP.
   d. At the command prompt, type `mount -o ro loop /tmp/System_Manager_06_03.iso /iso`.
   e. At the command prompt, type `cd /iso` and verify if the following files are present in the `iso` folder:
      - `pre-install.war` (war file)
      - `System_Manager_06_03.tar` (tar file)
      - `System_Manager_06_03_Post_Deploy.tar` (tar file)
      - `SystemManager.mf` (mf file)
      - `SystemManager.ovf` (ovf file)
2. To log on to System Platform Web Console, in the Web browser, type `https://`*`<IPAddress>`*, where *<IPAddress>* is the IP address of the C-dom Web Console.
3. Log on to System Platform Web Console using the administrator credentials made available at the time of the System Platform installation.
4. In the left navigation pane, click **Virtual Machine Management** > **Templates**.
5. Click **Install**.
6. On the Search Local and Remote Template page, select an appropriate installation mode.

   Note:

   You can download the installation files from the PLDS website or extract the installation files from the ISO image of the installer, and store the files at different locations. The locations depend on the mode of deploying the System Manager template. For more information on selecting a template, see Search Local and Remote Template field descriptions section in Installation methods on page 41.
7. To search the installation OVF file, click **Search**.

8. In the **Select Template** field, click the `SystemManager.ovf` file, and then click **Select**.
9. On the Select Template page, click **Continue without EPW file**.
10. On the Templates Details page, click **Install**.

    The installation starts and after the completion of the Pre-Install Web Application Deployment install phase, the system displays the Network Settings page.
11. On the Network Settings page, in the **IP Address** field, enter the IP address of the virtual machine on which you install System Manager.

    This IP address must be different from the IP address of the C-dom and Dom–0 virtual machines.
12. In the **Hostname** field, enter the short host name of the virtual machine, for example, `sp01smgr`.

    ✱ **Note:**

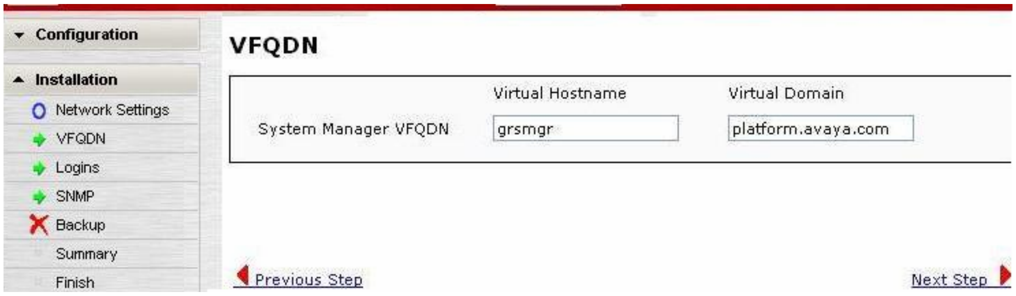
    If the host name contains a whitespace between the characters, for example, `sp01 smgr`, the installation fails. However, if the host name has a whitespace before the first character or after the last character, the system removes the whitespace and proceeds with the installation.
13. In the **Domain** field, enter the domain name of the virtual machine.
14. Click **Next Step**.
15. On the VFQDN page, the system displays default values in the following fields:

    a. In the **Virtual Hostname** field, enter a unique hostname.

    b. In the **Virtual Domain** field, enter a unique domain name.

    ✱ **Note:**

    - You can modify the host name and the domain.
    - The virtual FQDN value must be unique and different from the FQDN value of System Manager.
    - Ensure that the host name and the domain name are unique and comply with the enterprise DNS and security rules.
    - If you require to configure Geographic Redundancy, ensure that the host name and the domain on the primary and secondary System Manager servers remain the same.

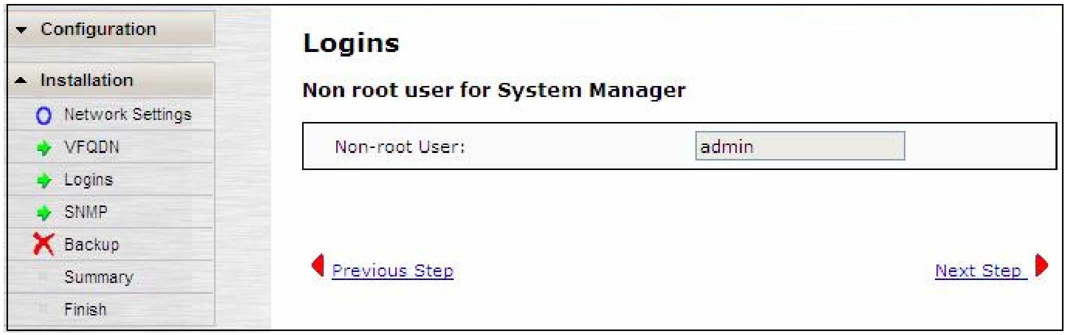


VFQDN

	Virtual Hostname	Virtual Domain
System Manager VFQDN	grsmgr	platform.avaya.com

16. To navigate to the Logins page, click **Next Step**.

    The system displays **admin** as the default value for the **Non-root User** field.

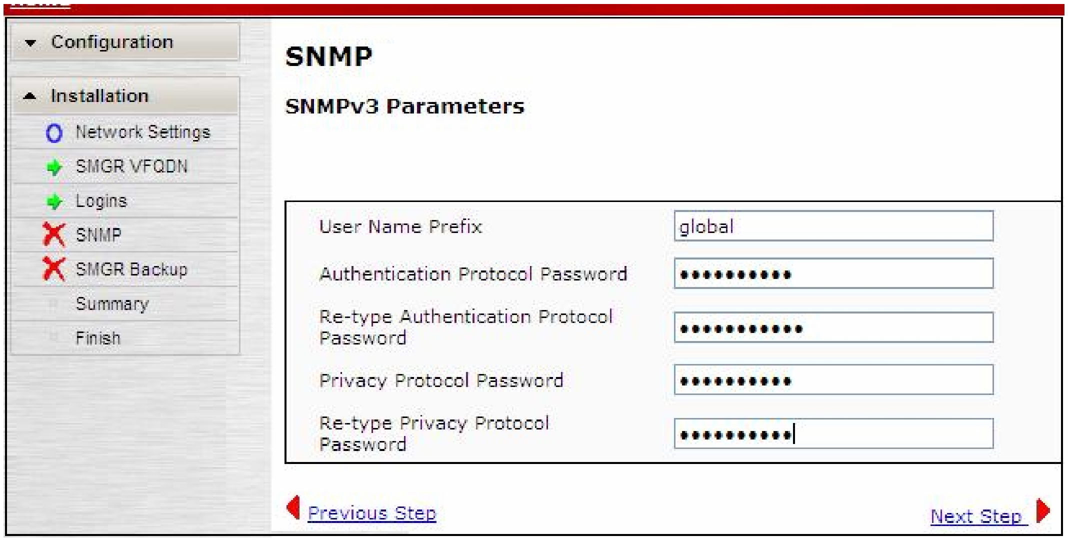


Logins

Non root user for System Manager

Non-root User: admin

17. Click **Next Step**.
18. On the SNMP v3 Parameters page, enter the appropriate values in the **User Name Prefix**, **Authentication Protocol Password**, and **Privacy Protocol Password** fields.

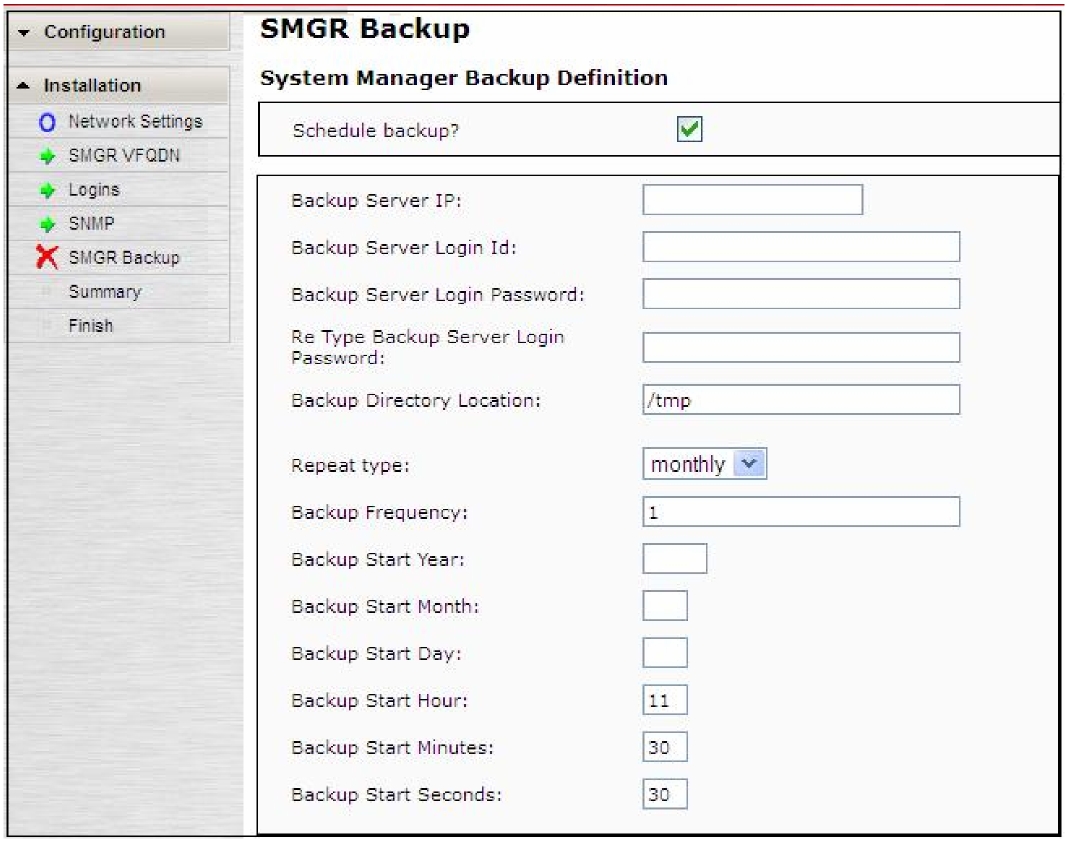


SNMP

SNMPv3 Parameters

User Name Prefix	global
Authentication Protocol Password	••••••••••
Re-type Authentication Protocol Password	•••••••••••
Privacy Protocol Password	••••••••••
Re-type Privacy Protocol Password	••••••••••

19. Click **Next Step**.
20. On the Backup page, select the **Schedule Backup?** check box and enter the details.



SMGR Backup

System Manager Backup Definition

Schedule backup? ☑

Backup Server IP:

Backup Server Login Id:

Backup Server Login Password:

Re Type Backup Server Login Password:

Backup Directory Location: /tmp

Repeat type: monthly

Backup Frequency: 1

Backup Start Year:

Backup Start Month:

Backup Start Day:

Backup Start Hour: 11

Backup Start Minutes: 30

Backup Start Seconds: 30

21. To view the Summary page, click **Next Step**.
22. To view the Confirm Installation page, click **Next Step**.
23. Select the **Accept License Terms?** check box.
24. Click **Install**.

    If you do not fill any of the mandatory fields in the installation steps, the system disables the **Install** button.

    Note:

    - See the System Manager Release 6.3 release note on the Avaya Support website at http://support.avaya.com for any post install patches that you must apply.
    - The installation process takes about 40–50 minutes to complete.

- During the execution of post install script, if the system does not display the progress, wait for the installation to complete.

Next steps

To gain access to System Manager Web Console, perform one of the following actions:

- In the Web browser, enter `https://<Fully qualified domain name of System Manager>`.
- On the System Platform Web Console, perform the following:
  a. Click **Home**.
  b. In the **Virtual Machine List** section, click the wrench icon (🔧) adjacent to the SMGR link.

     The system opens the System Manager login page.

To configure the system as secondary System Manager, see the instructions in the “Geographic Redundancy” section from *Administering Avaya Aura® System Manager*.

Installing System Manager using a DVD

Procedure

1. Insert the DVD in the DVD drive of the server.
2. Log on to the System Platform Web Console.
3. In the left navigation pane, click **Virtual Machine Management** > **Templates**.
4. Click **Install**.
5. Select **SP CD/DVD**.
6. To search the installation OVF file, click **Search**.
7. In the **Select Template** field, click the `SystemManager.ovf` file, and then click **Select**.
8. On the Select Template page, click **Continue without EPW file**.
9. On the Templates Details page, click **Install**.

   The installation starts and after the completion of the Pre-Install Web Application Deployment install phase, the system displays the Network Settings page.
10. On the Network Settings page, in the **IP Address** field, enter the IP address of the virtual machine on which you install System Manager.

    This IP address must be different from the IP address of the C-dom and Dom–0 virtual machines.
11. In the **Domain** field, enter the domain name of the virtual machine.

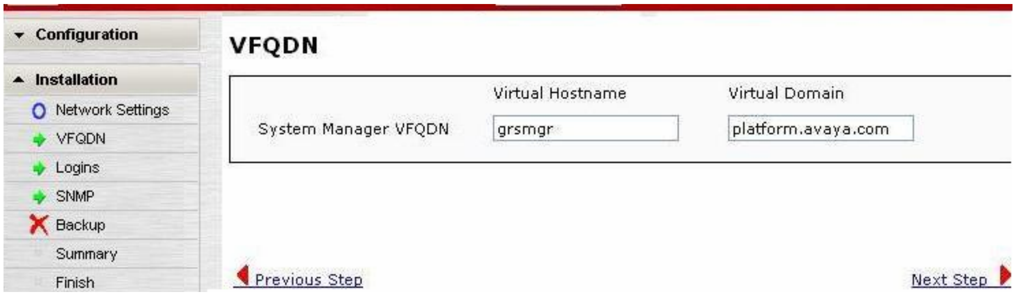
12. On the VFQDN page, the system displays default values in the following fields:

    a. In the **Virtual Hostname** field, enter a unique hostname.

    b. In the **Virtual Domain** field, enter a unique domain name.

    Note:

    - You can modify the host name and the domain.
    - The virtual FQDN value must be unique and different from the FQDN value of System Manager.
    - Ensure that the host name and the domain name are unique and comply with the enterprise DNS and security rules.
    - If you require to configure Geographic Redundancy, ensure that the host name and the domain on the primary and secondary System Manager servers remain the same.

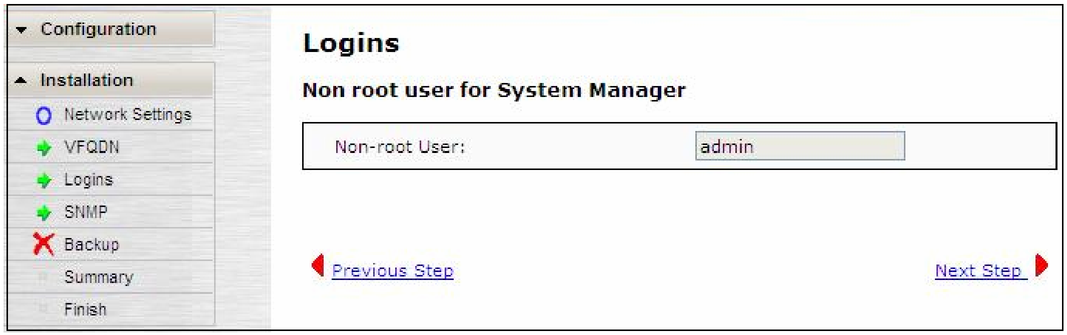


VFQDN

	Virtual Hostname	Virtual Domain
System Manager VFQDN	grsmgr	platform.avaya.com

13. To navigate to the Logins page, click **Next Step**.

    The system displays **admin** as the default value for the **Non-root User** field.

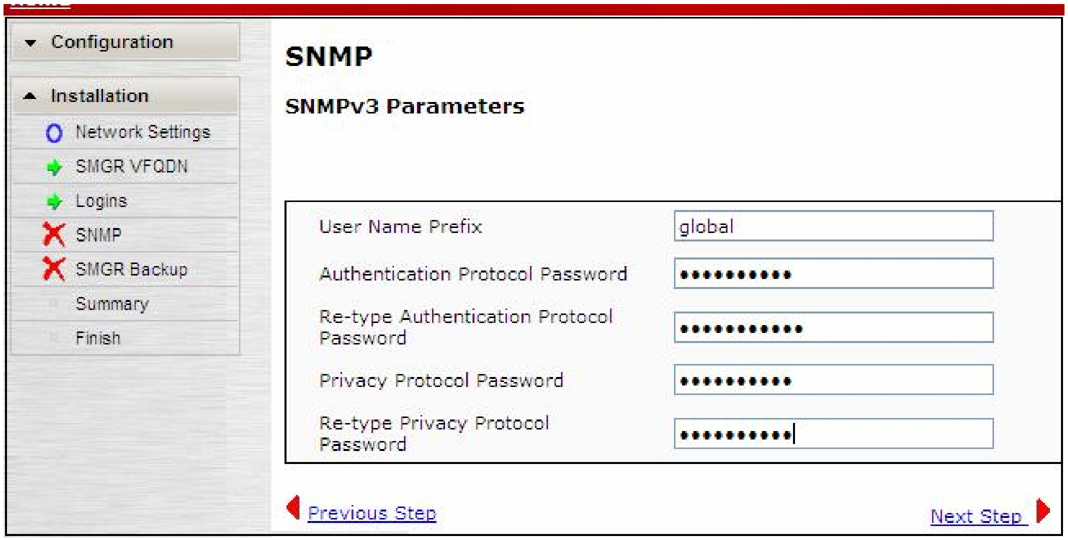


Logins

Non root user for System Manager

Non-root User: admin

14. On the SNMP v3 Parameters page, enter the appropriate values in the **User Name Prefix**, **Authentication Protocol Password**, and **Privacy Protocol Password** fields.

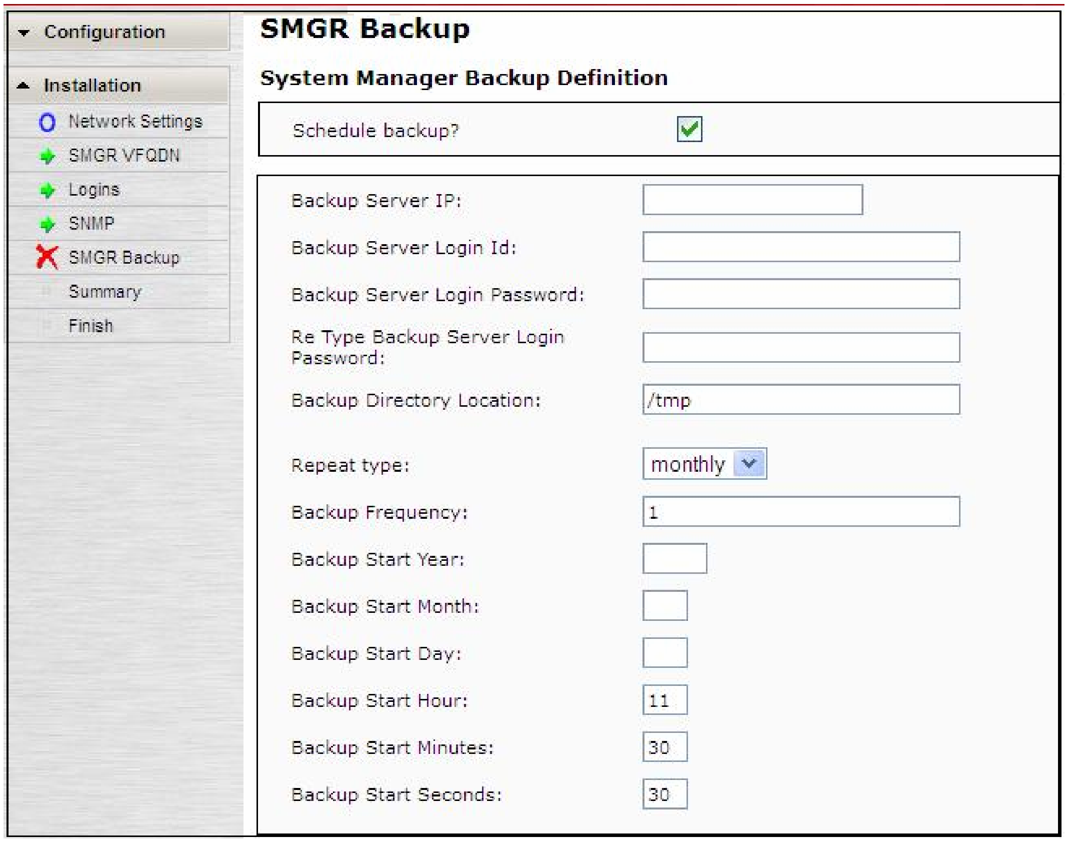


SNMP

SNMPv3 Parameters

User Name Prefix	global
Authentication Protocol Password	••••••••••
Re-type Authentication Protocol Password	•••••••••••
Privacy Protocol Password	••••••••••
Re-type Privacy Protocol Password	••••••••••

15. Click **Next Step**.
16. On the Backup page, select the **Schedule Backup?** check box and enter the details.



SMGR Backup

System Manager Backup Definition

Schedule backup? ☑

Backup Server IP:	
Backup Server Login Id:	
Backup Server Login Password:	
Re Type Backup Server Login Password:	
Backup Directory Location:	/tmp
Repeat type:	monthly
Backup Frequency:	1
Backup Start Year:	
Backup Start Month:	
Backup Start Day:	
Backup Start Hour:	11
Backup Start Minutes:	30
Backup Start Seconds:	30

17. To view the Summary page, click **Next Step**.
18. To view the Confirm Installation page, click **Next Step**.
19. Select the **Accept License Terms?** check box.
20. Click **Install**.

    If you do not fill any of the mandatory fields in the installation steps, the system disables the **Install** button.

    Note:

    - See the System Manager Release 6.3 release note on the Avaya Support website at http://support.avaya.com for any post install patches that you must apply.
    - The installation process takes about 40–50 minutes to complete.
    - During the execution of post install script, if the system does not display the progress, wait for the installation to complete.

Default credentials

Accessing the System Manager command line interface

You do not require the non-root user during the installation of the System Manager template. The system automatically uses admin. You can ssh to the virtual appliance using admin as the user name and password. You can change the login to root using the command **`su -`**.

Use root01 as the password. Change the default password when you log in for the first time.

Accessing the System Manager common Web console

To gain access to System Manager common Web console, open the URL `https://Fully qualified domain name of System Manager` in the Web browser. The default user name and password for gaining access to System Manager common Web console is admin and admin123. You must change the default password when you log in for the first time.

Using the System Manager Trap Listener service

Using the Trap Listener service, System Manager can receive SNMPv2c and SNMPv3 traps and informs from Avaya devices. Trap listener is configured with default values for SNMPv2c and SNMPv3 parameters. You can change these parameters after you install System Manager. The default value of the community string for SNMPv2c is an empty string. This means that System Manager receives SNMPv2c traps with any community string.

Note:

To change the default values for the Trap Listener from the System Manager Web Console, navigate to **Services** > **Configurations** > **Settings** > **SMGR** > **Trap Listener**.

After you change the Trap Listener settings, as an administrator, create a new SNMP Target profile for System Manager IP address, and a new SNMPv3 user profile for System Manager.

The values in the profiles must match the values in the Trap Listener settings. You must also attach the SMGR SNMPv3 user profile to the SMGR Target profile, and then attach the target profile to all the Serviceability Agents. For information on creating SNMP User and Target profiles and attaching the Target profiles to Serviceability Agents, see “Managing Serviceability Agents” in *Administering Avaya Aura® System Manager*.

Installing and committing the patches

Downloading patches

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Download/Upload**.
3. On the Search Local and Remote Patch page, select from the following locations to search for a patch.
    - **Avaya Downloads (PLDS)**
    - **HTTP**
    - **SP Server**
    - **SP CD/DVD**
    - **SP USB Disk**
    - **Local File System**
4. If you selected **HTTP**, enter the patch URL.

    Click **Configure Proxy** to specify a proxy server if required.
5. If you selected **SP Server**, copy the patch into System Platform server directory **/vsp-template**:
6. If you selected **Local File System**, click **Add** to locate the service pack file on your computer and then upload.
7. Click **Search** to search for the required patch.
8. Choose the patch and click **Select**.

Prerequisites for installing System Manager patches in the Geographic Redundancy setup

Ensure that you perform the following before you install the software patches on System Manager that is configured for Geographic Redundancy.

- Obtain the required System Manager software patch from PLDS website at http://support.avaya.com and copy the file to the computer.
- Disable the Geographic Redundancy replication on the primary System Manager server.
- Verify that the system displays the Geographic Redundancy status as disabled on top of System Manager Web Console.
- Create a backup of the System Manager data on the system and save the data on an external device.

Related topics:

Creating a backup of the System Manager data through System Platform on page 116

Installing patches

Before you begin

- To install a service pack as part of an installation, make sure that all applications or virtual machines are fully installed and functional.
- Download the patches your system requires.
- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:

    a. System Platform service packs

    b. System Platform feature pack

    c. Solution template service packs

    d. Solution template feature pack

About this task

Perform the following steps to install all System Platform and solution template service packs and feature packs by means of the System Platform Web Console.

Procedure

1. Click **Server Management** > **Patch Management** .
2. Click **Manage**.

The Patch List page displays the list of patches and the current status of the patches.

3. On the Patch List page, click on a patch ID to see the details.
4. On the Patch Detail page, click **Install**.

Configuring a proxy

About this task

If patches are located on a different server (for example, Avaya PLDS or HTTP), and depending on your network setup, configure a proxy address and port if necessary.

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Upload/Download**.
3. On the Search Local and Remote Patch page, click **Configure Proxy**.
4. On the System Configuration page, select **Enabled** for the **Proxy Status** field.
5. Specify the proxy address.
6. Specify the proxy port.
7. Select the appropriate keyboard layout.
8. Enable or disable statistics collection.
9. Click **Save** to save the settings and configure the proxy.

Committing patches

Before you begin

You have completed the following tasks using the Web Console:

- Downloading patches on page 111 (finding and downloading the particular patch you must install)
- Configuring a proxy on page 113 (if the patches are located in a different server)
- Installing patches on page 112 (for the particular patch you must install)

About this task

Use the following procedure to commit patches to the Avaya Aura® solution template Virtual Machine (VM). After you commit a patch, you cannot roll it back.

Note:

If you have patches to install separately on the System Platform and on an Avaya Aura® solution template, install the System Platform patch(es) first.

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.
   The Server Management Patch List page appears.
3. Click the patch that you must commit.
   The Web Console displays the Server Management Patch Detail page.
4. Click **Commit**.
   The Server Management Patch Detail page displays an in-progress message, for example: `Patch <patch_id> is being committed. Please wait....`
   The Patch Detail page then displays a completion message, for example: `Patch <patch_id> has been successfully committed`, or, `Failed to commit patch`.

Rolling back patches

About this task

Use this procedure to roll back patches to the solution template Virtual Machine (VM).

Note:

If you have patches to install separately on both System Platform and on the solution template, install the System Platform patches first.

Procedure

1. Click **Server Management** > **Patch Management**.
2. Click **Manage**.
   The Server Management Patch List page appears.
3. Click the patch that you want to roll back.
   The Web Console displays the Server Management Patch Detail page.
4. Click **Rollback**.
   The Server Management Patch Detail page displays an in-progress message, for example: `Patch <patch_id> is being rolled back. Please wait....`
   The Patch Detail page then displays a completion message, for example: `Patch`

`<patch_id> has been successfully rolled back`, or, `Failed to roll back patch`.

Feature packs

Avaya delivers feature packs in either RPM (patch) or ISO (full upgrade) format. Install or uninstall them as follows:

- RPM patch—From the Patch Management page of the System Platform Web Console.
- ISO image—From the appropriate (System Platform or Avaya Aura® product) installation wizard.

Feature packs have installation requirements that vary. For this reason, always see your solution documentation for specific prerequisites and installation instructions.

Guidelines for RPM-based feature packs

For any RPM-based feature pack associated with System Platform, the following installation guidelines apply:

- If your server is already running the latest version of System Platform available just prior to the feature pack release, install the RPM patch containing the feature pack.
- If your server is not running the latest version of System Platform available just prior to the feature pack release:
    a. Upgrade to the latest version of System Platform (including service packs) available just prior to the feature pack release.
    b. Install the RPM patch containing the feature pack.

Guidelines for ISO-based feature packs

For any ISO-based feature pack associated with System Platform, only the following guideline applies:

- Use the feature pack ISO image to perform a platform upgrade on the server.

Feature Pack installation process

If you are planning to install a new feature pack on your existing solution template, you must first meet System Platform requirements including platform upgrades, service pack installations, and any earlier feature packs if required. For example, with Communication Manager 6.0 running on System Platform 6.0, and with System Platform and Communication Manager each having a new FP1, the solution upgrade sequence is as follows:

1. Upgrade System Platform from version 6.0 to version 6.2.1.
2. Install RPM-based Feature Pack 1 for System Platform 6.2.1. This step brings System Platform to version 6.2.2.

3. Upgrade Communication Manager from version 6.0 to version 6.2.
4. Install Service Pack 4 for Communication Manager 6.2.

High availability configurations

If you are deploying an Avaya Aura® system in a System Platform High Availability configuration, the same installation or upgrade sequence applies to both the primary and secondary servers in the High Availability configuration.

Feature Pack installation

Use the installation method that is appropriate for the type of feature pack: RPM-based feature packs or ISO-based feature packs.

RPM-based feature packs

For RPM-based feature packs (for example, FP1 for System Platform 6.2.1), proceed to Patch management.

ISO-based feature packs

For ISO-based feature packs (for example, FP2 for a future major or minor version of System Platform), perform a platform upgrade. (See relevant topics in your Avaya Aura® solution documentation.)

Creating a backup of the System Manager data through System Platform

Before you begin

- Log on to System Platform Web Console.

About this task

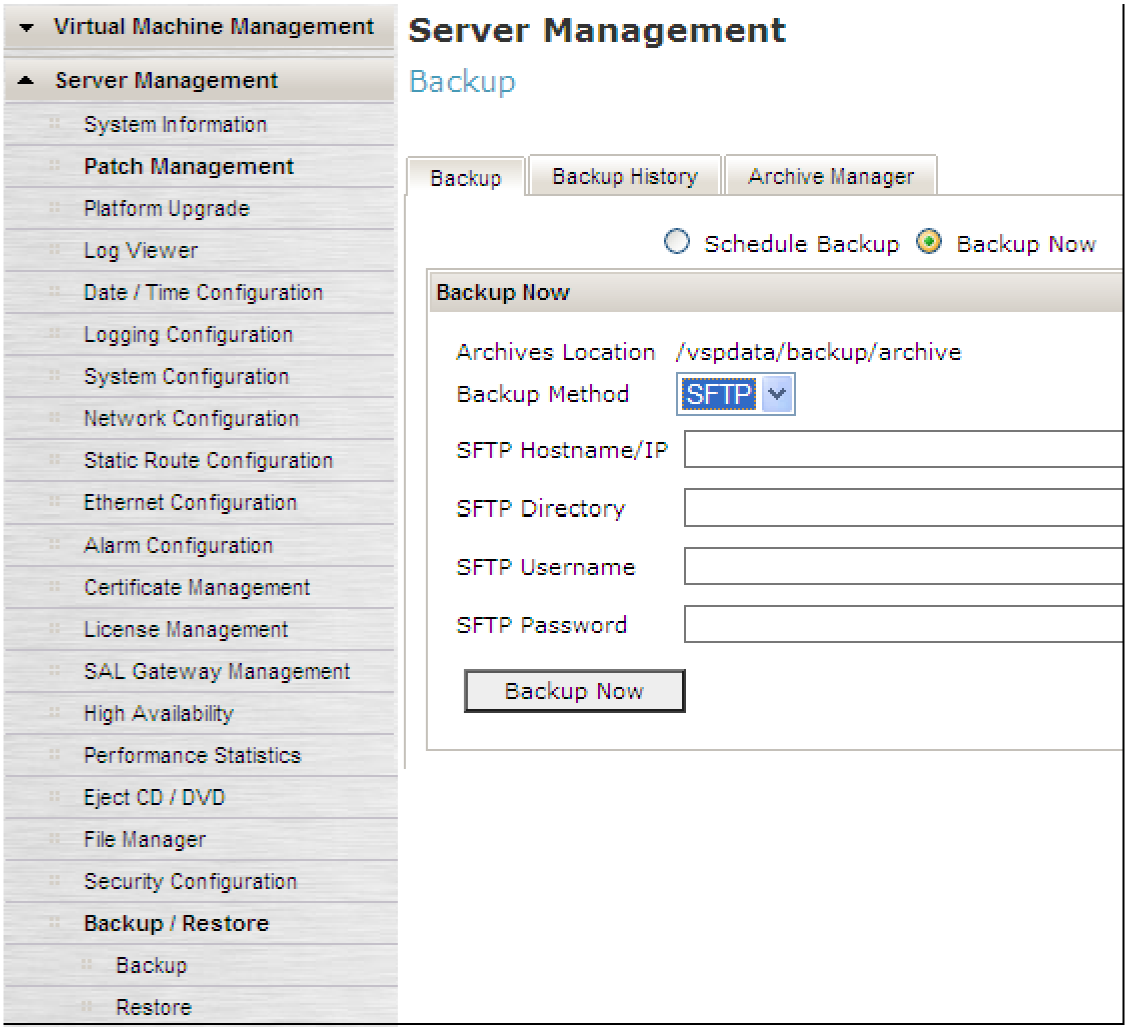
Important:

The backup file size can reach 3 GB. Ensure that you have that much free space at the location where you are storing the backup archive.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Backup**.
3. On the Backup page, select the **Backup Now** option to start the backup operation immediately.

4. In the **Backup Method** field, click `SFTP`.



Server Management

Backup

○ Schedule Backup ● Backup Now

Backup Now

Archives Location /vspdata/backup/archive

Backup Method SFTP

SFTP Hostname/IP

SFTP Directory

SFTP Username

SFTP Password

5. Enter the information in the following fields:
   - **SFTP Hostname/IP**
   - **SFTP Directory**
   - **SFTP Username**
   - **SFTP Password**

   The system saves the backup archive file on the designated SFTP host server and on the System Platform server.

6. Click **Backup Now**.

   Note:

   Contact Avaya Support at http://support.avaya.com/ if:

   - You need to repeatedly terminate a backup operation manually.

- System Platform automatically terminates a backup operation because of system errors.

The backup progress window opens in the Backup tab and displays backup event messages with corresponding timestamps. The window remains open until any of the following events occur:

- The operation concludes successfully.
- You manually terminate the operation.
- A system error condition abruptly halts the operation.

Related topics:
Recommendations for System Manager data backup on page 119

Creating a data backup on a remote server

Procedure

1. Perform one of the following:
   - For System Manager 6.1 and later, on System Manager Web Console, click **Services** > **Backup and Restore**.
   - For System Manager 6.0, on System Manager Web Console, click **System Manager Data** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Remote**.
4. Specify the remote server IP, remote server port, user name, password, and name and path of the backup file that you create.
5. Click **Now**.
   If the backup is successful, the Backup and Restore page displays the message: `Backup job submitted successfully. Please check the status detail below!!`

Related topics:
Recommendations for System Manager data backup on page 119

Recommendations for System Manager data backup

You can create a backup of the System Manager data using one of the following methods:

1. Using System Manager Web Console to backup System Manager configuration files and the System Manager database.
2. Using System Platform Web Console to backup System Platform data and System Manager data.

However, use System Platform to create the System Manager backup in the following scenarios:

- Restoring the System Manager and System Platform data
- Upgrading System Manager and System Platform
- Cold Standby for System Manager

Installing patches on System Manager servers configured for Geographic Redundancy

Before you begin

Obtain the required System Manager software patch from PLDS website at http://support.avaya.com and copy the file to the computer on which you installed System Manager.

Procedure

1. Log on to System Manager Web Console of the primary System Manager, disable the Geographic Redundancy replication. For instructions, see Disabling the Geographic Redundancy replication.
   If the system disables the Geographic Redundancy replication successfully, System Manager Web Console displays the status `GR - Disabled`.
2. Create a backup of the System Manager data on the system and save the data on an external device. For instructions, see Creating a backup of the System Manager data through System Platform.
3. On the primary System Manager server, install the System Manager patch:
   a. Log on to System Platform that corresponds to the primary System Manager.
   b. Install the software patch for System Manager. For instructions, see Installing patches.
   c. To verify the version, log on the primary System Manager, click **About**.

The system displays the latest patch details of System Manager.

   d. Log on to System Platform Web Console, click **Commit**.

4. On the secondary System Manager server, install the System Manager patch:
   a. Log on to System Platform that corresponds to the secondary System Manager.
   b. Install the software patch for System Manager. For instructions, see Installing patches.
   c. To verify the version, log on the secondary System Manager, click **About**.
      The system displays the latest patch details of System Manager.

      Note:

      The version of the System Manager software must be the same on the primary and the secondary server.
   d. Log on to System Platform Web Console, click **Commit**.
5. Log on to System Manager Web Console of the primary System Manager, enable the Geographic Redundancy replication. For instructions, see Enabling the Geographic Redundancy replication.
   If the system enables the Geographic Redundancy replication successfully, System Manager Web Console displays the status `GR – Enabled`.
6. To verify the Geographic Redundancy setup, perform the following steps:
   a. Click **Administators** > **Elements**.
   b. Click on the secondary System Manager server link.

      The system must log you on to the secondary System Manager server without you entering the password.

Appendix B: System Manager installation checklist

#	Action	Notes	✔
1	Verify that the RAID Controller battery level is not low. If the battery level is low, replace the battery before you proceed with the upgrade.	**Important:** If the RAID Controller battery depletes, the Disk Cache policy is set to WriteThrough. As a result, the overall system operations slow down and the duration of the upgrade process increases. For additional information, see the S8800 or HP ProLiant DL360 G7 server RAID on the Avaya Support website at http://support.avaya.com/.	
2	Download the following software from the Avaya Product Licensing and Delivery System (PLDS) at https://plds.avaya.com: • The System Platform Release 6.3.0.0.18002 software • The System Manager template from the System_Manager_06_03..iso file • The `System_Manager_R6.3_FP2_S4_1399.bin` file	Verify that the md5sum for the downloaded ISO image matches the number on the PLDS website.	
3	Set up a DVD or a USB flash drive to install System Platform from a DVD or USB flash drive.		
4	The two System Manager servers must meet the requirements that are defined in Prerequisites for servers in the Geographic Redundancy setup.		

Appendix C: System Manager information worksheet

In the System Manager template deployment, you must fill in several fields using System Platform Web Console. Print the following tables and work with your network administrator to fill in the appropriate value for each field displayed in these tables.

System Manager virtual appliance

Field	Value	Notes
IP Address		IP address that you must assign to the System Manager virtual appliance on System Platform.
Hostname		Short hostname for System Manager. For example, smgrmachine.
Domain		Fully qualified domain name for System Manager. For example, mydomain.com.
Virtual FQDN		grsmgr+<domain name>, the virtual FQDN for System Manager that is set in a Geographic Redundancy system. You can change the domain name to a unique name. The virtual FQDN value must be unique and different from the FQDN value of System Manager.
User Name Prefix		Prefix for the user name. Using this prefix you can create six SNMPv3 users, one for each of the SNMPv3 authentication and privacy protocol combination, and store the users in the System Manager database.
Authentication Protocol Password		Authentication password for the six SNMPv3 users that you create.
Privacy Protocol Password		The SNMPv3 privacy password for the six SNMPv3 users that you create.
Backup Definition		The details required to schedule automatic remote backup.

Appendix D: Compatibility matrix for the System Manager and System Platform software versions

System Manager		System Platform	
Release	Build number	Release	Required patch
5.2	• 2.0.8.0 • 2.0.8.1 if you installed patch 1 for System Manager 5.2.	1.1.1.0.2	1.1.1.4.2
5.2 SP1	2.0.9.0	1.1.1.0.2	1.1.1.4.2
5.2 SP2	2.0.9.3	1.1.1.0.2	1.1.1.97.2
6.0	• 6.0.0.0.556-3.0.6.0 • 6.0.0.0.556-3.0.6.1 if you installed the `SystemManager_06_00_Patch_01.sh` patch. • 6.0.0.0.556-3.0.6.2 if you installed the `SystemManager_06_00_Patch_02.sh` patch.	6.0.0.0.11	-
6.0 SP1	• 6.0.0.0.668-3.0.7.0 • 6.0.0.0.668-3.0.7.1 if you installed the `SystemManager_06_00_SP1_Patch_01.bin` patch.	6.0.0.0.11	-
6.0 SP2	6.0.0.0.668-3.0.7.2	6.0.0.0.11	-
6.1	• 6.1.0.4.5072-6.1.4.11 • 6.1.0.4.5072-6.1.4.62	6.0.2.0.5	-
6.1 SP0	6.1.0.4.5072-6.1.4.113	6.0.2.0.5	6.0.2.6.5
6.1 SP1.1	6.1.0.0.7345-6.1.5.9	6.0.3.0.3	-
6.1 SP2	6.1.0.0.7345-6.1.5.106 and software update 6.1.6.1.1087	6.0.3.0.3	-

System Manager		System Platform	
Release	Build number	Release	Required patch
6.1 SP3	6.1.0.0.7345-6.1.5.112 and software update 6.1.7.1.1260	6.0.3.0.3	-
6.1 SP4	6.1.0.0.7345-6.1.5.115 and software update 6.1.8.1.1455 or 6.1.8.1.1551	6.0.3.0.3	-
6.1 SP5	6.1.0.0.7345-6.1.5.502 and software update 6.1.9.1.1634	6.0.3.0.3	6.0.3.6.3
6.1 SP6	6.1.0.0.7345-6.1.5.606 and software update 6.1.10.1.1774	6.0.3.0.3	6.0.3.6.3
6.1 SP7	6.1.0.0.7345-6.1.5.702 and software update 6.1.11.1.1860	6.0.3.0.3	6.0.3.7.3
6.1 SP8	6.1.0.0.7345-6.1.5.803) software update 6.1.12.1.1906	6.0.3.0.3	6.0.3.10.3
6.2	6.2.0.0.15669-6.2.12.9 and software update 6.2.12.1.1822	6.2.0.0.27	-
6.2 SP1	6.2.0.0.15669-6.2.12.105 and software update 6.2.13.1.1871	6.2.0.0.27	6.2.0.2.27
6.2 SP2	6.2.0.0.15669-6.2.12.202 and software update 6.2.14.1.1925	6.2.1.0.9	-
6.2 SP3	6.2.0.0.15669-6.2.12.307 and software update 6.2.15.1.1959	6.2.1.0.9	6.2.1.3.9
6.2 SP4	6.2.0.0.15669-6.2.12.307 and software update 6.2.16.1.1993	6.2.1.0.9	6.2.1.3.9
6.3	6.3.0.8.5682-6.3.8.818 and software update 6.3.0.8.923	6.2.1.0.9	6.2.2.06002.0
6.3 SP1	6.3.0.8.5682-6.3.8.859 software update 6.3.1.9.1212	6.2.1.0.9	6.2.2.08001.0

Appendix E: System Manager and System Platform patches

To upgrade System Manager to Release 6.3.x, install System Platform and System Manager patches in the following sequence for a release:

System Manager release	System Platform and System Manager patches	Notes
6.3 SP1 Software-upgrade only	1. Upgrade System Platform from Release 6.2.2.08001.0 to 6.3.0.0.18002. 2. Install the `System_Manager_R6.3_FP2_S4_1399.bin` file.	
6.3 Software-upgrade only	1. Upgrade System Platform from Release 6.2.2.06002.0 to 6.3.0.0.18002. 2. Install the `System_Manager_R6.3_FP2_S4_1399.bin` file.	
6.2 SP3 or SP4 Software-upgrade only	1. Upgrade System Platform from Release 6.2.1.3.9 to 6.3.0.0.18002. 2. Upgrade System Manager to 6.3. 3. Install the `System_Manager_R6.3_FP2_S4_1399.bin` file.	
6.2 SP2 Software-upgrade only	1. Upgrade System Platform from Release 6.2.1.0.9 to 6.3.0.0.18002. 2. Upgrade System Manager to 6.3. 3. Install the `System_Manager_R6.3_FP2_S4_1399.bin` file.	
6.2 SP1 Software-upgrade only	1. Upgrade System Platform Release 6.2.0.2.27 to 6.3.0.0.18002. Upgrade System Manager to 6.3. 2. Install the `System_Manager_R6.3_FP2_S4_1399.bin` file.	

System Manager release	System Platform and System Manager patches	Notes
6.2 Software-upgrade only	1. Upgrade System Platform Release 6.2.0.0.27 to 6.3.0.0.18002. 2. Upgrade System Manager to 6.3. 3. Install the `System_Manager_R6.3_FP2_S4_1399.bin` file.	
6.2, 6.2 SP1, SP2, SP3, or SP4 Hardware and software upgrades	1. Install System Platform Release 6.3.0.0.18002. 2. Install the System Manager 6.2 template and 6.2 SP1, SP2, SP3, or SP4. 3. Upgrade System Manager to 6.3. 4. Install the `System_Manager_R6.3_FP2_S4_1399.bin` file.	
6.1 SP1.1	1. On the new server, install System Platform Release 6.3.0.0.18002. 2. Install the System Manager 6.1 SP1.1 template. 3. Install the `System_Manager_06_01_patch.sh` preupgrade patch on System Manager 6.1 SP1. 4. Upgrade System Manager to 6.3. 5. Install the `System_Manager_R6.3_FP2_S4_1399.bin` file.	
6.1	1. Install the preupgrade patch `System_Manager_06_01_SP0_r873.bin`. 2. On the new server, install System Platform Release 6.3.0.0.18002. 3. Install the System Manager 6.1 template. 4. Install the `System_Manager_06_01_SP0_r873.bin` patch. 5. Install the `System_Manager_06_01_patch.sh` preupgrade patch. 6. Upgrade System Manager to 6.3. 7. Install the `System_Manager_R6.3_FP2_S4_1399.bin` file.	

System Manager release	System Platform and System Manager patches	Notes
6.0 SP1	1. On the new server, install System Platform Release 6.3.0.0.18002. 2. Install the `SystemManager_06_00_SP1_Patch_01.bin` patch on System Manager 6.0 SP1. 3. Install the `SystemManager_06_00_SP1_Patch_02.bin` patch on System Manager 6.1 SP1. 4. Upgrade System Manager to 6.3. 5. Install the `System_Manager_R6.3_FP2_S4_1399.bin` file.	
6.0	1. Install the preupgrade patches `SystemManager_06_00_SP1_Patch_01.bin` and `SystemManager_06_00_SP1_Patch_02.bin` on System Manager 6.0 SP1. 2. On the new server, install System Platform Release 6.3.0.0.18002. 3. Install the `SystemManager_06_00_Patch_01.bin` and `SystemManager_06_00_Patch_02.bin` patches on System Manager 6.0 SP1. 4. Install the `SystemManager_06_00_SP1_Patch_01.bin` patch. 5. Upgrade System Manager to 6.3. 6. Install the `System_Manager_R6.3_FP2_S4_1399.bin` file.	
5.2 SP1	1. On the new server, install System Platform Release 1.1.1.0.2. 2. Install System Platform 1.1.1.97.2. 3. Install System Manager 5.2 SP1 on System Platform. 4. Upgrade System Platform to Release 6.0.2.0.5. 5. Install the System Platform 6.0.2.6.5 patch. 6. Upgrade System Manager to 6.0 SP1.	

System Manager release	System Platform and System Manager patches	Notes
	7. Install the `SystemManager_06_00_SP1_Patch_01.bin` patch. 8. Upgrade System Platform to Release 6.0.3.0.3. 9. Install the System Platform 6.0.3.9.3 patch. 10. Upgrade System Platform from Release 6.0.3.9.3 to 6.3.0.0.18002. 11. Upgrade System Manager to 6.3. 12. Install the `System_Manager_R6.3_FP2_S4_1399.bin` file.	
5.2	1. Install the preupgrade patch `System_Manager_05_02_GA_Patch_01.zip`. 2. On the new server, install System Platform Release 1.1.1.0.2. 3. Install System Platform 1.1.1.97.2. 4. Install System Manager 5.2 on System Platform. 5. Install the `System_Manager_05_02_GA_Patch_01.zip` patch. 6. Upgrade System Platform to Release 6.0.2.0.5. 7. Install the System Platform 6.0.2.6.5 patch. 8. Upgrade System Manager to 6.0 SP1. 9. Install the `SystemManager_06_00_SP1_Patch_01.bin` patch. 10. Upgrade System Platform to Release 6.0.3.0.3. 11. Install the System Platform 6.0.3.9.3 patch. 12. Upgrade System Platform from Release 6.0.3.9.3 to 6.3.0.0.18002. 13. Upgrade System Manager to 6.3. 14. Install the `System_Manager_R6.3_FP2_S4_1399.bin` file.	

Index