Upgrading Avaya Aura® System Manager to the latest 6.3.x release on System Platform

Release 6.3
Issue 5
August 2016

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 may generally make available to users of its products and Hosted Services. 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 Avaya hardware and software. 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 or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. 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 CHANNEL PARTNER; 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. “Software” means Avaya’s computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. “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. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type

Designated System(s) License (DS). End User may install and use each copy or an Instance 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, Instance, 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”, or such successor site as designated by Avaya. 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, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, 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 product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel 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 or Hosted Service 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”). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

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 or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya, the Avaya logo, Avaya Aura® System Manager are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

This document contains upgrading checklists and procedures.

Intended audience

This document is intended for people who perform upgrades.

Document changes since last issue

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

- Added step to install the Release 6.3.8 bin file on System Manager 6.3.0, run the datamigration utility, and then install the Release 6.3.18 bin file.
- Updated the datamigration overivew section.
- Added procedure for installing the System Manager Release 6.3.18 bin file.
- Added support for running the data migration process in the background.
- Updated the Upgrading System Manager by using the data migration utility procedure.
- Removed the Installing the System Platform 6.3.4.08007.0 patch procedure.
- Updated the System Manager and System Platform patches section.
- Updated Compatibility matrix for the System Manager and System Platform software versions.

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			
	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
-	Deploying Avaya Aura® System Manager on VMware® in the Virtualized Environment.	Describes the procedures for deploying the Avaya Aura® System Manager virtual application in the Avaya Aura® Virtualized Environment.	Implementation Engineers and Support personnel
	Installing the Dell™ PowerEdge™ R620 server	Describes the procedures to install the Dell™ PowerEdge™ R620 server.	Implementation Engineers and Support personnel
	Installing the HP ProLiant DL360p G8 server	Describes the procedures to install the HP ProLiant DL360p G8 server.	Implementation Engineers and Support personnel
	Installing and Configuring System Platform	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	Implementation Engineers and

Table continues…

Document number	Title	Description	Audience
		System Manager and the managed elements that System Manager supports.	Support personnel
	Upgrading Avaya Aura® System Platform	Describes the procedures to upgrade System Platform and the Services virtual machine from the earlier releases to the latest release.	
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
1A00234E	Avaya Aura® Fundamental Technology	AvayaLive™ Engage Theory
1A00236E	Knowledge Access: Avaya Aura® Session Manager and System Manager Fundamentals	AvayaLive™ Engage Theory
5U00106W	Avaya Aura® System Manager Overview	WBT Level 1
4U00040E	Knowledge Access: Avaya Aura®Session Manager and System Manager Implementation	ALE License
5U00050E	Knowledge Access: Avaya Aura®Session Manager and System Manager Support	ALE License
5U00095V	Avaya Aura® System Manager Implementation, Administration, Maintenance, and Troubleshooting	vILT+Lab Level 1
5U00097I	Avaya Aura®Session Manager and System Manager Implementation, Administration, Maintenance, and Troubleshooting	vILT+Lab Level 2
3102	Avaya Aura® Session Manager and System Manager Implementation and Maintenance Exam	Exam (Questions)
5U00103W	Avaya Aura® System Manager 6.2 Delta Overview	WBT Level 1

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to 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 website.

Note:

Videos are not available for all products.

Support

Go to 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.

Chapter 2: Upgrade overview and considerations

System Manager upgrades

This document provides the procedures for upgrading Avaya Aura® System Manager from earlier releases to System Manager Release 6.3.18 running on System Platform.

You can upgrade System Manager to Release 6.3.18 by using one of the following methods:

- Data migration utility: To upgrade System Manager from Release 6.x:
  1. If 6.x is earlier than 6.3, deploy the 6.0 OVA file.
  2. If 6.3.x is earlier than 6.3.8, install the 6.3.8 bin file.
  3. Run the data migration utility from the command line interface.
  4. Install the Release 6.3.18 bin file.

  Data migration utility is the preferred method of System Manager upgrade.
- Network Routing Policy (NRP) export and import utility: To upgrade System Manager from Release 5.2.x, on the 5.2.x system, export the routing data using the NRP export utility and then import the routing data using the NRP import utility to Release 6.3.18.
- System Platform web console: To upgrade from earlier releases to Release 6.3.18, use the System Platform web console to install the software required for the release.

  Note:

  If your system is running System Manager Release 6.0 or earlier, upgrade to 6.0 SP1 by using the 6.0 SP1 procedures that are available on the Avaya support site before you upgrade to the latest System Manager Release 6.3.x.

For procedures to upgrade to System Manager Release 6.3.18 running on VMware, see *Upgrading Avaya Aura® System Manager on VMware in Virtualized Environment*.

Important:

- Use the document to upgrade to the latest System Manager release. For the latest available System Manager release, see “Compatibility matrix for the System Manager and System Platform software versions” or the latest System Manager 6.3.x release notes on the Avaya support site.

- The latest System Manager release is cumulative of earlier 6.3.x releases. For example, if 6.3.18 is the latest System Manager release, 6.3.18 is cumulative of 6.3.1, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.6, 6.3.7, 6.3.8, 6.3.9, 6.3.10, 6.3.11, 6.3.12, 6.3.13, 6.3.14, 6.3.15, 6.3.16, and 6.3.17.
- The target release mentioned in this document is Release 6.3.18. However, to upgrade to the latest release available for System Manager, use the appropriate System Manager bin file. For more information, see “Compatibility matrix for the System Manager and System Platform software versions” or the latest System Manager 6.3.x release notes on the Avaya support site.

Related links

Compatibility matrix for the System Manager and System Platform software versions on page 22

Supported servers

System Manager supports the following servers for upgrades to Release 6.3.18:

- Avaya S8800 1U
- Dell™ PowerEdge™ R610 2CPU MID2
- HP ProLiant DL360 G7 2CPU MID4
- Dell™ PowerEdge™ R620
- HP ProLiant DL360p G8

If you must change the server, use Dell™ PowerEdge™ R620 or HP ProLiant DL360p G8 to install System Platform and System Manager.

Chapter 3: Planning for upgrade

Prerequisites for servers on System Platform in the Geographic Redundancy setup

In a Geographic Redundancy setup, ensure that the two standalone System Manager servers that you designate as primary and secondary servers meet the following requirements:

- Must contain the same hardware such as Dell™ PowerEdge™ R620 server.
- Must have the same hardware configuration, for example, the same processor.
- Must contain the same version of the System Platform software that includes software packs.

  Note:

  System Manager does not support the mixed VMware and System Platform environment. For example, the primary System Manager on and the secondary System Manager on VMware ESXi.
- Must contain the same version of the System Manager software that includes service pack and software patches.
- Must contain the same parent domain names for two System Manager systems. For example, smgr.abc.com and smgr.xyz.com are invalid domain names because the parent domain names abc and xyz are different.
- Must be able to communicate with each other over the network using the IP address and FQDN.
- Must have synchronized network time.
- Must use DNS to ensure that the name resolution is automatic. Otherwise, you must resolve the IP address and the host name in the `/etc/hosts` file on the primary and secondary System Manager servers.
- Must ensure that the required ports are open to support the Geographic Redundancy feature. For port usage information, see *Avaya Port Matrix: Avaya Aura® System Manager* on the Avaya Support website at http://support.avaya.com/.
- Must ensure that the minimum data pipe between the primary and the secondary System Manager server is T1. T1 provides 1.544 Mbps.
- Must ensure that the network latency is less than 500 ms.

System Manager and System Platform patches

Download the System Manager and System Platform patches from the Avaya Support website. For information about version compatibility, see Compatibility matrix for the System Manager and System Platform software versions.

Note:

If your system is running System Manager Release 6.0 or earlier, upgrade to 6.0 SP1 by using the 6.0 SP1 procedures that are available on the Avaya support site before you upgrade to System Manager Release 6.3.

Note:

For detailed instructions to complete each task, see the relevant section in this document.

To upgrade System Manager 6.0 SP1 or later to Release 6.3.18, install System Platform and System Manager patches in the following sequence for a release:

System Manager release	System Platform and System Manager patches	Notes
6.3.0, 6.3 SP1, 6.3.2 through 6.3.16. Hardware and software upgrades	1. On the new server, install System Platform Release 6.3.7.0.05001. 2. Install the System Manager Release 6.3 template. 3. Install the `System_Manager_6.3.18_r5505487.bin` file.	
6.3.0, 6.3 SP1, 6.3.2 through 6.3.16. Software-upgrade only	1. Upgrade System Platform to 6.3.7.0.05001. 2. Install the `System_Manager_6.3.18_r5505487.bin` file.	
6.2 SP1, SP2, SP3 or SP4 Software-upgrade only	1. Upgrade System Platform to 6.3.7.0.05001. 2. Upgrade System Manager to Release 6.3. 3. Install the `System_Manager_6.3.18_r5505487.bin` file.	
6.2, 6.2 SP1, SP2, SP3, or SP4	1. On the new server, install System Platform release that is compatible with 6.2, 6.2 SP1, SP2, SP3, or SP4. Get the Release 6.2.x compatible software from the Avaya support site.	

Table continues…

System Manager release	System Platform and System Manager patches	Notes
Hardware and software upgrades	2. Install the System Manager 6.2 template and 6.2 SP1, SP2, SP3, or SP4 as appropriate. 3. Install System Platform Release 6.3.7.0.05001. 4. Upgrade System Manager to Release 6.3. 5. Install the `System_Manager_6.3.18_r5505487.bin` file.	
6.1 SP2, SP3, SP4, SP5, SP6, SP7, or SP8	1. On the new server, install System Platform release that is compatible with 6.1 SP2, SP3, SP4, SP5, SP6, SP7, or SP8. Get the Release 6.1.x compatible software from the Avaya support site. 2. Install the System Manager 6.1 SP1.1 template. 3. Upgrade System Manager to 6.1 SP2, SP3, SP4, SP5, SP6, SP7, or SP8. 4. Upgrade System Platform to Release 6.3.7.0.05001. 5. Install the System Manager Release 6.3 template. 6. Install the `System_Manager_6.3.18_r5505487.bin` file.	
6.1 SP1.1	1. On the new server, install System Platform release that is compatible with 6.1 SP1.1. Get the Release 6.1.x compatible software from the Avaya support site. 2. Install the System Manager 6.1 SP1.1 template. 3. Install the `System_Manager_06_01_patch.sh` preupgrade patch. 4. Upgrade System Platform to Release 6.3.7.0.05001. 5. Install the System Manager Release 6.3 template. 6. Install the `System_Manager_6.3.18_r5505487.bin` file.	
6.1	1. On the new server, install System Platform release that is compatible with 6.1. Get the Release 6.1.x compatible software from the Avaya support site. 2. Install the System Manager 6.1 template. 3. Install the `System_Manager_06_01_SP0_r873.bin` file. 4. On System Manager 6.1 SP1, install the `System_Manager_06_01_patch.sh` preupgrade patch file. 5. Upgrade System Platform to Release 6.3.7.0.05001. 6. Install the System Manager Release 6.3 template.	

Table continues…

System Manager release	System Platform and System Manager patches	Notes
	7. Install the `System_Manager_6.3.18_r5505487.bin` file.	
6.0 SP2	1. On the new server, install System Platform release that is compatible with 6.0 SP2. Get the Release 6.1.x compatible software from the Avaya support site. 2. Install the System Manager 6.0 SP1 template. 3. Install the `System_Manager_06_00_SP2_r820.bin` file. 4. Upgrade System Platform to Release 6.3.7.0.05001. 5. Install the System Manager Release 6.3 template. 6. Install the `System_Manager_6.3.18_r5505487.bin` file.	
6.0 SP1	1. On the new server, install System Platform release that is compatible with 6.0 SP1. Get the Release 6.1.x compatible software from the Avaya support site. 2. Install the System Manager 6.0 SP1 template. 3. Install the `SystemManager_06_00_SP1_Patch_01.bin` patch on System Manager 6.0 SP1. 4. Install the `SystemManager_06_00_SP1_Patch_02.bin` patch on System Manager 6.1 SP1. 5. Upgrade System Platform to Release 6.3.7.0.05001. 6. Install the System Manager Release 6.3 template. 7. Install the `System_Manager_6.3.18_r5505487.bin` file.	

Compatibility matrix for the System Manager and System Platform software versions

The following table provides the software version of System Platform that is compatible with the System Manager version for a release.

System Manager			System Platform	
Release	Required bin file	Build number	Release	Required patch
6.3.0	System Platform based:	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

Table continues…

System Manager			System Platform	
Release	**Required bin file**	**Build number**	**Release**	**Required patch**
	System_Manager_06_03.iso Virtualized Environment based: SMGR-6.3.0.8.5682-e50-64.ova			
6.3 SP1	System_Manager_06_03_ServicePack1_r1212.bin	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
6.3.2	System_Manager_6.3.2_r1399.bin	6.3.0.8.5682-6.3.8.1627 and software update 6.3.2.4.1399	6.3.0.0.18002	-
6.3.3	System_Manager_6.3.3_r2501719.bin	6.3.0.8.5682-6.3.8.1814 software update 6.3.1.9.1719	6.3.0.0.18002	-
6.3.4	System_Manager_6.3.4_r3401830.bin	6.3.0.8.5682-6.3.8.2631 software update 6.3.4.4.1830	6.3.0.0.18002	6.3.1.08002.0
6.3.5	System_Manager_6.3.5_r3501969.bin	6.3.0.8.5682-6.3.8.2807 software update 6.3.5.5.1969	6.3.0.0.18002	6.3.1.08002.0
6.3.6	System_Manager_6.3.6_r3602103.bin	6.3.0.8.5682-6.3.8.3007 software update 6.3.6.6.2103	6.3.0.0.18002	6.3.1.08002.0
6.3.7	System_Manager_6.3.7_r3702275.bin	6.3.0.8.5682-6.3.8.3204 software update 6.3.7.7.2275	6.3.0.0.18002	6.3.1.08002.0
6.3.8	System_Manager_6.3.8_r4502376.bin	6.3.0.8.5682-6.3.8.4219 software update 6.3.8.5.2376	6.3.0.0.18002	6.3.1.08007.0
6.3.9	System_Manager_6.3.9_r4602482.bin	6.3.0.8.5682-6.3.8.4414 software update 6.3.9.1.2482	6.3.0.0.18002	6.3.1.08007.0
6.3.10	System_Manager_6.3.10_r4702656.bin	6.3.0.8.5682-6.3.8.4514 Software Update Revision No: 6.3.10.7.2656	6.3.0.0.18002	6.3.5.01003.0
6.3.11	System_Manager_6.3.11_r4802871.bin	6.3.0.8.5682-6.3.8.4711 Software Update Revision No: 6.3.11.8.2871	6.3.0.0.18002	6.3.5.01003.0
6.3.12	System_Manager_6.3.12_r4903022.bin	6.3.0.8.5682-6.3.8.4903 Software Update Revision No: 6.3.12.9.3022	6.3.0.0.18002	6.3.5.01003.0

Table continues…

System Manager			System Platform	
Release	**Required bin file**	**Build number**	**Release**	**Required patch**
6.3.13	`System_Manager_6.3.13_r5003336.bin`	6.3.0.8.5682-6.3.8.5108 Software Update Revision No: 6.3.13.10.3336	6.3.0.0.18002	6.3.6.01005.0
6.3.14	`System_Manager_6.3.14_r5103595.bin`	6.3.0.8.5682-6.3.8.5304 Software Update Revision No: 6.3.14.11.3595	6.3.7.0.05001	Not applicable
6.3.15	`System_Manager_6.3.15_r5203972.bin`	6.3.0.8.5682-6.3.8.5506 Software Update Revision No: 6.3.15.12.3972	6.3.7.0.05001	Not applicable
6.3.16	`System_Manager_6.3.16_r5304210.bin`	6.3.0.8.5682-6.3.8.5709 Software Update Revision No: 6.3.16.13.4210	6.3.7.0.05001	Not applicable
6.3.17	`System_Manager_6.3.17_r5404616.bin`	6.3.0.8.5682-6.3.8.5810 Software Update Revision No: 6.3.17.14.4616	6.3.7.0.05001	6.3.8.01002.0

System Manager upgrades checklist

Serial Number	Action	Notes	✔
1	Check the RAID Controller battery level. 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 DL360p G8 server RAID on the Avaya Support website at http://support.avaya.com/.	
2	Verify the software version on System Manager from the **About** link of the web console or run the **`swversion`** command.	-	
3	Download the following software from the Avaya Support website at http://support.avaya.com to the `/tmp` file: • System Platform Release 6.3.7.0.05001 • The System Manager template if required	Verify that the md5sum for the downloaded System Platform ISO image and the System Manager template matches the number on the Avaya Support website.	

Table continues…

Serial Number	Action	Notes	✔
	• The `System_Manager_6.3.18_r5505487.bin` file and required System Manager preupgrade patches	For the list of System Platform and System Manager patches that you must install for a release, see theSystem Manager and System Platform patches section.	
4	For a server upgrade, download and install aDell R620 server or an HP DL360 G8 server.	For instructions, see *Installing the Dell™ PowerEdge™ R620 Server* or *Installing the HP ProLiant DL360p G8 Server*.	
5	Create a backup of System Manager, System Platform, and the Services virtual machine.	See the appropriate backup procedures.	
6	Ensure that the two System Manager servers meet the requirements that are defined in Prerequisites for servers in the Geographic Redundancy setup.	-	
7	In the High Availability (HA) setup, stop HA on the active and standby System Manager servers.	See High Availability start/stop.	
8	In the Geographic Redundancy setup, disable the replication between the primary and secondary System Manager servers.	See *Administering Avaya Aura® System Manager*.	
9	Install System Platform Release 6.3.7.0.05001.	Installing System Platform on page 55	
10	(Optional) Upgrade the Services virtual machine to version 3.0 if you are upgrading from System Platform Release 6.2.x.	See *Upgrading Avaya Aura®System Platform*.	
11	Restore the backup of System Manager, System Platform, and the Services virtual machine.	Restoring the System Manager backup data on page 177	
12	Install the System Manager template if required.	Installing the System Manager template on page 161	
13	Install the `System_Manager_6.3.18_r5505487.bin` file. The patch installation takes about 65–70 minutes to complete on the primary and the secondary System Manager server.	Installing the System Manager Release 6.3.18 bin file on page 164	
14	Commit the patch installation.		
15	To get the updated kernel that is running in the memory, restart System Manager	-	
16	Verify that the upgrade is successful.	Verifying the functionality of System Manager on page 259	

Table continues…

Serial Number	Action	Notes	✔
17	In the High Availability (HA) setup, start HA on the active and standby System Manager servers.	See High Availability start/stop.	
18	In the Geographic Redundancy setup, enable the replication between the primary and secondary System Manager servers.	See *Administering Avaya Aura® System Manager*.	

Related links

Prerequisites for servers on System Platform in the Geographic Redundancy setup on page 19

System Manager information worksheet

During the System Manager template deployment, from the System Platform web console, you must fill in several fields. 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		The IP address that you must assign to the System Manager virtual appliance on System Platform.
Hostname		The short hostname for System Manager. For example, smgrmachine.
Domain		The 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		The 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		The 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.

Installation worksheet for System Platform

Use the System Platform preinstallation worksheet to help you gather in advance vital configuration values for successful installation, and for initial administration immediately following installation.

The System Platform installer application requires you to fill in various fields. Having the values required for these fields in advance helps the installation to progress more efficiently and accurately. It is likewise important and useful to gather information in advance about other key fields important for System Platform administration immediately following installation.

Print out the following tables and work with your network administrator to fill in the rows.

System Configuration

Name	Value	Description
Proxy Configuration:		
Status		Specifies whether an http proxy should be used to access the Internet, for example, when installing templates, upgrading patches, or upgrading platform.
Address		The address for the proxy server.
Port		The port address for the proxy server.
Cdom Session Timeout		
Session Timeout Status		Specifies whether Cdom session timeout is enabled or disabled.
Session Timeout (minutes)		The maximum time in minutes that a Cdom session remains open after the last user transaction with the System Platform Web Console or Cdom CLI.
WebLM Configuration:		
SSL		Specifies whether the Secure Sockets Layer (SSL) protocol will be used to invoke the WebLM server. Select **Yes** if the alternate WebLM application has an HTTPS web address. Otherwise, select **No** if the alternate WebLM application has an HTTP web address. Default value = **Yes**.
Host		The IP address or host name extracted from the web address of

Table continues…

Name	Value	Description
		the WebLM application. Default value = <*cdom_IP_address*>.
Port		The logical port number extracted from the web address of the WebLM application, for example, `4533`. Default value = `52233`
Other System Configuration:		
Syslog IP Address		IP address of the Syslog server, which collects log messages generated by the System Platform operating system.
Keyboard Layout		Determines the specified keyboard layout for the keyboard attached to the System Platform server.
Statistics Collection		If you disable this option, the system stops collecting the statistics data. **Note:** If you stop collecting statistics, the system-generated alarms will be disabled automatically.
SNMP Discovery		By default, this feature enables SNMPv2 management systems to automatically discover any System Platform server in an Avaya Aura® based network, including retrieval of server status and vital statistics. This is useful, for example, when using System Manager to view the entire inventory of System Platform servers across multiple Avaya Aura® enterprise solutions at a glance. This feature eliminates the tedious and error-prone task of manually adding extra System Platform servers to an SNMP management system, where that system often requires three or more IP addresses for each System Platform server. SNMP management systems can also query any recognized System

Table continues…

Name	Value	Description
		Platform server for the logical server configuration. System Platform supports network discovery of values for the following MIB objects: • RFC 1213 (MIB-2, autodiscovery): sysDescr, sysObjectID, sysUpTime, sysContact, sysName, sysLocation, and sysServices • RFC 2737 (Entity MIB) get/getnext/getbulk: entPhysicalTable – One table entry for the Dom0 physical interface. entLogicalTable – One table entry for the Cdom virtual machine, and one table entry for each virtual machine associated with the installed solution template. Each entry contains the virtual machine name, type, software version, and IP address. If you disable this option, SNMP manager systems will be unable to automatically discover this System Platform server.

Enable IPv6 Configuration

Name	Value	Description
Turn On IPv6		Enables IPv6.

General Network Settings Configuration

Name	Value	Description
Default Gateway		The default gateway IP address.
Primary DNS		The primary Domain Name System (DNS) server address.
Secondary DNS		(Optional) The secondary DNS server address.
Domain Search List		The search list, which is normally determined from the local domain

Table continues…

Name	Value	Description
		name. By default, it contains only the local domain name. You can change this by listing the domain search path that you want following the *search* keyword, with spaces or tabs separating the names.
Cdom 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.
Dom0 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.
Physical Network Interface		The physical network interface details for eth0 and eth1 (and eth2 if High Availability Failover is enabled).
Domain Dedicated NIC		Applications with high network traffic or time-sensitive traffic often have a dedicated NIC. This means the virtual machine connects directly to a physical Ethernet port and usually requires a separate cable connection to the customer network.

Table continues…

Name	Value	Description
		See template installation topics for more information.
Bridge		The bridge details for the following: • **avprivate**: This is called a private bridge because it does not use any Ethernet interface, so it is strictly internal to the server. The System Platform installer attempts to assign IP addresses that are not in use. • **avpublic**: This bridge uses the Ethernet interface associated with the default route, which is usually eth0, but can vary based on the type of the server. This bridge usually provides access to the LAN for System Platform elements (System Domain (Dom-0) and Console Domain) and for any guest domains that are created when installing a template. The IP addresses specified during System Platform installation are assigned to the interfaces that System Domain (Dom-0) and Console Domain have on this bridge. • **template bridge**: These bridges are created during the template installation and are specific to the virtual machines installed.
Domain Network Interface		The domain network interface details for System Domain (Dom-0) or Console Domain that are grouped by domain based on your selection.
Global Template Network Configuration		The set of IP addresses and host names of the applications hosted on System Platform. Also includes the gateway address and network mask.

Table continues…

Name	Value	Description
VLAN		Required only when installing System Platform on the S8300D server.

Services Virtual Machine Configuration

Name	Value	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 (checkmark) for remote access and local SAL support, or disabled (no checkmark) 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 assigned to the Services Virtual Machine
Static IP address		The IP address assigned to the Services Virtual Machine. The address must be on the same subnetwork 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.

Ethernet Configuration

Name	Value	Description
Speed		Sets the speed in MB per second for the interface. Options are: • 10 Mb/s half duplex

Table continues…

Name	Value	Description
		• 10 Mb/s full duplex • 100 Mb/s half duplex • 100 Mb/s full duplex • 1000 Mb/s full duplex Auto-Negotiation must be disabled to configure this field.
Port		Lists the available Ethernet ports. Auto-Negotiation must be disabled to configure this field.
Auto-Negotiation		Enables or disables autonegotiation. By default it is enabled, but might cause some problems with some network devices. In such cases you can disable this option.

Bonding Interface Configuration

Name	Value	Description
Name		Is a valid bond name. It should match regular expression in the form of “bond[0-9]+”.
Mode		Is a list of available bonding modes that are supported by Linux. The available modes are: • Round Robin • Active/Backup • XOR Policy • Broadcast • IEEE 802.3ad • Adaptive Transmit Load Balancing • Adaptive Load Balance For more information about bonding modes, see http://www.linuxhorizon.ro/bonding.html.

Table continues…

Name	Value	Description
		Note: The default mode of new bonding interface is Active/Backup.
Slave 1/Primary		Is the first NIC to be enslaved by the bonding interface. If the mode is Active/Backup, this will be the primary NIC.
Slave 2/Secondary		Is the second NIC to be enslaved by the bonding interface. If the mode is Active/Backup, this will be the secondary NIC.

Static Route Configuration

Note:

A network restart or VM reboot is necessary to enable static route updates in the web console.

Name	Value	Description
Interface		The bridge through which the route is enabled.
Network Address		The IP address of a destination network associated with an Avaya (or Avaya Partner) remote services host.
Network Mask		The subnetwork mask for the destination network.
Gateway		The address of a next-hop gateway that can route System Platform traffic to or from a remote services host on the destination network.

SNMP Trap Receiver Configuration

Name	Value	Description
Product Id		Product ID for System Platform Console Domain. 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.

Table continues…

Name	Value	Description
		Note: VSPU is the model name for Console Domain.
IP Address		IP address of the trap receiver.
Port		Port number on which traps are received.
Community		SNMP community to which the trap receiver belongs. Must be `public`.
Device Type		Default setting is **INADS**. Do not change this settings.
Notify Type		Default setting is **TRAP**. Do not change this setting.
Protocol Version		Default setting is **V2c**. Do not change this setting.

Password Configuration

Note:

Passwords must be at least six characters long. Use uppercase and lowercase alphabetic characters and at least one numeral or special character.

Name	Value	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. The cust login is for audit purposes. It has read-only access to the Web Console, except for changes to its password, and no command line access.
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.

Network Time Protocol Configuration

Name	Value	Description
NTP server 1		The host name or IP address of an NTP server, visible in the Web Console when you click **Query State** in the Date and Time Configuration page, under **Server Management**. When displayed, either of the following special characters precede each server host name or IP address. Each character has a special meaning, as follows: • Asterisk character (*): The preferred server (referenced by the local system), chosen by System Platform. • Plus character (+): Indicates a high-quality candidate for the reference time that System Platform can use if the selected time source becomes unavailable. Avaya preconfigures several server names before system delivery. You can add more NTP reference servers by clicking **Add** in the Date and Time Configuration page under **Server Management**.
NTP server 2		
NTP server 3		
NTP server 4		

Cdom and network interface configuration for System Platform High Availability configurations

Name	Value	Description
Remote cdom IP address		IP Address of Console Domain on the standby node.
Remote cdom user name		User name for Console Domain on the standby node.
Remote cdom password		Password for Console Domain on the standby node.

Table continues…

Name	Value	Description
Primary network interface		Network interface connected to the customer network.
Crossover network interface		Network interface connected to the standby server.

Ping targets configuration

Name	Value	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.

Checking the RAID Controller Battery state

Before you begin

Log on to the System Platform web console using admin credentials.

Procedure

1. Click **Server Management** > **Log Viewer**.
2. Select **System Logs**.
3. Select **Critical/Fatal** as the log level.
4. In the **Find** field, type `O_AVDM` and click **Search**.
5. Search for `O_AVDM10101`, `O_AVDM10102`, or `O_AVDM10100` in the **Message Content** column of the result table.

   If the alarm is present, you must replace the raid battery of the system.

Checking the RAID controller and RAID battery status

Before you begin

Log in to System Platform Dom-0 as root.

Procedure

1. To get the server name, type the following command:

   ```
   # dmidecode -s system-product-name
   ```

   The system displays the server type, for example, ProLiant DL360 G8.

2. Type the following commands:

   ```
   # cd /usr/sbin
   # ./hpacucli controller all show details
   ```

   The system displays the details of the server.

3. Perform one of the following:

   - Do not replace the RAID battery, if the system displays the following message:

     ```
     ..........................
     Accelerator Ratio: 25% Read / 75% Write
     Drive Write Cache: Disabled
     ........................
     ........................
     Battery/Capacitor Count: 1
     Battery/Capacitor Status: OK
     ```

   - Replace the RAID battery, if the system displays the following message:

     ```
     ..........................
     Accelerator Ratio: 100% Read / 0% Write
     ........................
     ........................
     Battery/Capacitor Count: 0
     ........................
     ```

Checking the RAID controller and RAID battery status on the S8800 server

Before you begin

Log in to System Platform Dom-0 as root.

Procedure

1. Type the following command:

   ```
   /opt/MegaRAID/MegaCLi/MegaCLi64 LDInfo LDall -a0
   ```

The command applies to the HP and Dell servers. The system displays the status of RAID controller and RAID battery.

2. Perform the following:
   - Do not replace the battery if the system displays the following message:

     ```
     Current Cache Policy: WriteBack, ReadAheadNone, Direct, No Write
     Cache if Bad BBU
     ```

   - If the system displays the following message, perform the next steps:

     ```
     Current Cache Policy: WriteThrough, ReadAheadNone, Direct, No
     Write Cache if Bad BBU
     ```

     WriteThrough indicates that the RAID battery might have a problem.

     a. To confirm the status of the battery, type the following command:

        ```
        /opt/MegaRAID/MegaCLi/MegaCLi64 adpbbucmd -a0 | more
        ```

     b. Note the following details:

        - **Max Error**: The value above 5 indicates that the battery has issue. The default is 2 %. 100% indicates that the battery is charging or discharging and also indicates that the RAID battery or RAID controller might have a problem.
        - **Remaining Capacity**: If the value reaches 400, change the battery.
        - **Design Capacity**: Depends on **Remaining Capacity**.

Chapter 4: Common procedures for System Manager upgrades

Overview

This chapter provides the common procedures that you must perform when you upgrade System Manager.

Tasks for software-only upgrades

Software-only upgrade of System Manager to Release 6.3.18 includes the following tasks:

1. Verifying the current version of System Manager.
2. Creating a backup of the System Manager data by usingSystem Platform.
3. Installing the latest System Platform patches.
4. Installing the preupgrade patch on System Manager, if applicable.
5. Upgrading System Platform to a release that is compatible with System Manager Release 6.3.
6. Upgrading the Services virtual machine to version 3.0.

   Perform this step only when you upgrade from System Platform Release 6.2.x.
7. Upgrading System Manager to Release 6.3.
8. Installing the `System_Manager_6.3.18_r5505487.bin` file.
9. Regenerating and reimporting third-party certificates, if you have used third-party certificates.
10. Verifying that System Manager functions correctly.

For detailed instructions to complete each task, see the relevant section in this document.

Related links

System Manager and System Platform patches on page 20

Tasks for hardware and software upgrades

Hardware and software upgrade of System Manager to Release 6.3.18 includes the following tasks:

1. Verifying the current version of System Manager.
2. Creating a backup of the System Manager data by usingSystem Platform.
3. Shutting down the existing server or removing the network connection.
4. Installing the new server.
5. On the new server, installing System Platform that is compatible with the release of the latest upgraded System Manager.
6. Installing the latest System Platform patches.
7. Installing the System Manager template of the current release.
8. Installing the preupgrade patch on System Manager, if applicable.
9. Restoring the System Manager data on the new system through System Platform.
10. Upgrading the Services virtual machine to version 3.0.

    Perform this step only when you upgrade from System Platform Release 6.2.x.
11. Upgrading System Manager to Release 6.3.
12. Installing the `System_Manager_6.3.18_r5505487.bin` file.
13. Regenerating and reimporting third-party certificates, if you have used third-party certificates.
14. Verifying that System Manager functions correctly.

For detailed instructions to complete each task, see the relevant section in this document.

Related links

System Manager and System Platform patches on page 20

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_Version_II.iso` file. The ISO file contains the following files:
     - `pre-install.war`
     - `System_Manager_06_03.tar`
     - `System_Manager_06_03._Post_Deploy.tar`
     - `System_Manager_06_03.gz`
     - `SystemManager.mf`
     - `SystemManager.ovf`

     You can also download these files individually from the same location.
   - The `System_Manager_6.3.18_r5505487.bin` file
10. On the About the Download Manager page, click **Click to download your file now**.
11. **(Optional)** If the system displays an error message about ActiveX installation, 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 with a check mark.

Downloading System Manager from the Avaya Support website

Procedure

1. On the web browser, type `http://support.avaya.com`.
2. Click **DOWNLOADS & DOCUMENTS**.
3. In the **Enter Your Product Here** field, enter **Avaya Aura® System Manager**.
4. In the **Choose Release** field, click **6.3.x**.
5. Select **Downloads** > **Enter**.

6. Download the following software to the `/tmp` folder on your computer:
   - The `System_Manager _06_03_Version_II.iso` file. The ISO file contains the following files:
     - `pre-install.war`
     - `System_Manager_06_03_Version_II.tar`
     - `System_Manager_06_03_Post_Deploy.tar`
     - `SystemManager.mf`
     - `SystemManager.ovf`

     You can also download these files individually from the Avaya Support website.
   - The `System_Manager_6.3.18_r5505487.bin` file.

Patch management

You can install, download, and manage the regular updates and patches for System Platform and the various templates provided by Avaya. Go to http://support.avaya.com and see the latest Release Notes for information about the latest patches.

You can install or download the patches from the Avaya Product Licensing and Delivery System (PLDS) website at http://plds.avaya.com.

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 URL to navigate to the patch.

If required, click **Configure Proxy** to specify a proxy server.

5. If you selected **SP Server**, copy the patch into PLDS server folder named **/vsp-template**.
6. If you selected **Local File System**, click **Add** to find the patch file on your computer and then upload.
7. Click **Search** to search for the required patch.

System Manager patch installation

Use one of the following procedures to install the System Manager patches:

- For System Manager releases earlier than 6.2, use the command line interface. For instructions, see Installing the System Manager patch using the command line interface.
- For System Manager Release 6.2 and later, use System Platform Web Console. For instructions, see Installing patches.

Related links

Installing patches on page 45
Installing the System Manager patch using the command line interface on page 44

Installing the System Manager patch using the command line interface

Before you begin

- Back up the System Manager data on the system, and save the data on an external device.
- Get the required System Manager software patch from the Avaya Support website at http://support.avaya.com. Copy the file to the computer on which you installed System Manager.
- Start an SSH session.

About this task

Use this procedure to install the software patch for System Manager releases earlier than 6.2. For System Manager 6.2 and later, use System Platform Web Console to install the software patch. For instructions, see Installing patches on page 45.

Procedure

1. Using the command line interface, log in to System Manager as `root`.
2. To provide permissions to run the file, go to the folder where you copied the System Manager patch.
3. Type `chmod +x <System_Manager_patch.in>`.

Where *System_Manager_patch.bin* is the System Manager software patch that you must install.

For example, for System Manager 6.1 SP1.1, you must install `System_Manager_06_01_SP1-1_r1030.bin`.

4. To run the System Manager patch, type `sh <System_Manager_patch.bin>`.

   Wait for the installer to complete running the patch.

5. Log on to System Manager Web Console and perform the following:
   a. Verify whether the system displays the System Manager Web Console correctly.
   b. In the upper-right corner, click **About** and verify the details of the patch.

Installing patches

Before you begin

- To install a service pack as part of an installation, ensure that all applications or virtual computers are fully installed and functional.
- Download the patches your system requires.

About this task

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

Note:

- Do not use the patch installers provided by your solution templates.
- Install patches in the following sequence:
  1. System Platform service packs
  2. System Platform feature packs
  3. Solution template service packs
  4. Solution template feature packs

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 a patch ID to view the details.
4. On the Patch Detail page, click **Install**.

Next steps

Commit the patch.

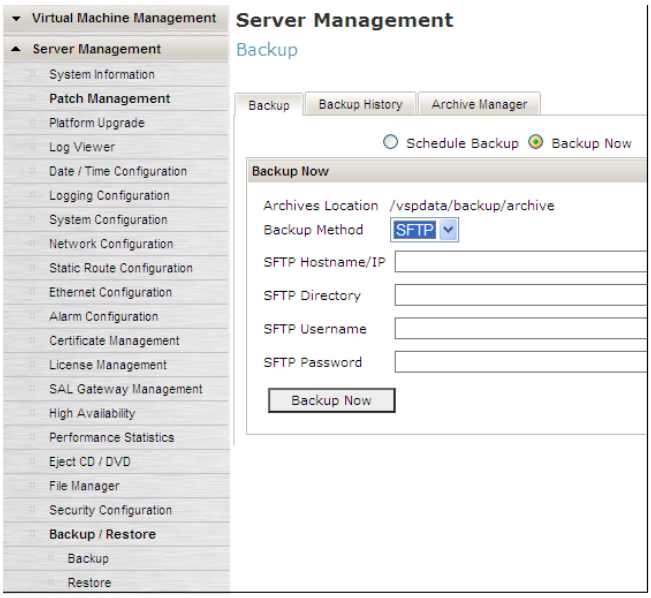
Creating a backup of the System Manager data through System Platform

Before you begin

Ensure that 3-GB free space is available at the location where you want to back up theSystem Manager data.

Procedure

1. Log on to System Platform web console.
2. Click **Server Management** > **Backup/Restore**.
3. Click **Backup**.
4. On the Backup page, select the **Backup Now** option to start the backup operation immediately.
5. In the **Backup Method** field, select `SFTP`.



6. Enter 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.
7. 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 links

System Manager data backup options on page 49

Backup progress window

Backup operations for some computers can be lengthy. As an administrative aid, System Platform displays a window to report progress information during a backup operation.

Backup progress monitoring

The backup progress window shows:

- Time-stamped progress messages from System Platform and applications running on local template virtual computers. This includes messages filtered directly from backup logs, for example, data set backup start, pause, end, or failure.
- A backup process countdown timer. The timer counts down until the operation ends successfully, halts because of errors or manual termination, or the estimated timer value expires. The countdown timer supplements the progress message content. Thus users can make a more informed decision about whether a problem occurred requiring a system recovery.

Backup progress monitoring runs automatically for the following operations:

- Manual backup
- Template upgrade backup

Backup progress warning and error messages

The progress window indicates whether a warning or error condition originated in System Platform or in a specific template computer, including:

- *Non-fatal warning* messages, such as:
  - A message reporting a normal event that requires no remedial action.
  - A message reporting a failure to back up a data set that is nonexistent.

- An unusually delayed series of progress messages on a particular template virtual computer suggests that the backup operation for that data set has a problem. In this case, choose either to continue the operation, or manually end the operation.

- *Fatal warning messages*—In the event of any critical backup error, the operation in progress immediately ends with a message describing the failure.

Note:

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

- You must repeatedly end a backup operation manually.
- System Platform automatically ends a backup operation because of system errors.

To aid in troubleshooting a failed system backup, you can get progress messages during the last backup from the Web Console Backup page.

Creating a data backup on a remote server

Procedure

1. On the 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:
     a. In the **File transfer protocol** field, click `SCP` or `SFTP`.
     b. Enter 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, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can 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 links

System Manager data backup options on page 49

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!!`

System Manager data backup options

To back up System Manager data, use one of the following methods:

1. Back up the System Manager configuration files and the System Manager database on System Manager Web Console.
2. Back up System Platform and System Manager data on System Platform Web Console.

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
- Changing over to the cold standby System Manager server

Note:

System Manager does not support the backup and restore operations from System Platform Web Console if System Manager is running on VMware.

Installing System Platform

Preinstallation tasks for System Platform

Preinstallation checklist for System Platform

Before starting System Platform installation, ensure 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 email button. See Registering the system on page 51.	**Important:** Submit the registration form three weeks before the planned installation date.	
2	Gather the required information about installation, such as IP configuration information, DNS addresses, and address information for Network Time Protocol (NTP) servers. See Installation worksheet for System Platform on page 27.		
3	Register for PLDS unless you have already registered. See Registering for PLDS on page 52.		
4	Download the System Platform installer ISO image file from PLDS. See Downloading software from PLDS on page 52.		
5	Download the appropriate solution template and licenses from PLDS. See Downloading software from PLDS on page 52.		
6	Verify that the downloaded ISO images match the images on the PLDS website. See Verifying the ISO image on a Linux-based computer on page 53 and Verifying the ISO image on a Windows-based computer on page 53.		

Table continues…

No.	Task	Notes	✔
7	Write the ISO images to separate DVDs. See Writing the ISO image to DVD or CD on page 54.	**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.

Avayaassigns a Solution Element ID (SE ID) and Product ID to each SAL Gateway and managed device that is registered. In System Platform, managed devices are the components of System Platform and of the applications 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 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 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. Gain access to the registration form and follow the instructions. The SAL registration form is available at http://support.avaya.com. In the Help & Policies section, click **More Resources**. The system displays the More Resources page. Click **Avaya Equipment Registration**, and search for *SAL Universal Install Form Help Document*.
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 come up
- Products in the solution template and supporting information as prompted by the form

Avayauses this information to register your system. When processing of the registration request is complete, Avaya sends you an email 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 links

Configuration prerequisites on page 81
SAL Gateway on page 80
Gateway Configuration field descriptions on page 84

Registering for PLDS

Procedure

1. Go to the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.

   The PLDS website redirects you to the Avaya single sign-on (SSO) webpage.

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 email 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 website.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Search for the available downloads using one of the following methods:
   - By download name
   - By selecting an application type from the drop-down list
   - By download type

   After entering the search criteria, click **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 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 check mark next to the downloads that have 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 file name`, where *file name* is the name of the ISO image. Include the .iso file name extension.
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. Do not use multiple rewrite DVDs which are prone to error.

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 can write 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 can write ISO images to CD.

Important:

When the ISO image is writing 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 59.

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 any more requirements of a specific Avaya Aura® solution template.

Note:

Because each Avaya Aura® solution template has different requirements for server resources, configuration, capacity, and performance, see 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 6.3 and the Services Virtual Machine (VM), and SAL Gateway registration and configuration.

If you are planning to install System Platform 6.3.4 and have already installed System Platform 6.3 on your system, install only the 6.3.4 feature pack.System Platform 6.3.4 is an RPM-based feature pack. See Feature Pack installation on page 119.

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 59. • Disable use of proxy servers in the Web browser on the laptop. See Disabling proxy servers in Microsoft Internet Explorer on page 60 or Disabling proxy servers in Mozilla Firefox on page 60 .		
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 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	Put the DVD in the DVD drive on the server. See Starting the installation from your laptop on page 61 or Starting the installation from the server console on page 62 depending on your selection of installation method.		

Table continues…

No.	Task	Notes	✔
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 62.		
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 61.		
8	Select the required keyboard type. See Selecting the type of keyboard on page 63.		
9	Verify the System Platform server hardware. See Verifying the System Platform server hardware on page 63.		
10	Verify that the image on the System Platform DVD is not corrupt. See Verifying the System Platform image on the DVD on page 64.		
11	Configure the network settings for the System Domain (Domain-0). See Configuring network settings for System Domain on page 65.		
12	Configure the network settings for the Console Domain. See Configuring network settings for Console Domain on page 67.		
13	Install the Services Virtual Machine (services_vm). See Installing the Services virtual machine on page 69.	**Important:** When the Services VM Network Configuration window displays 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	

Table continues…

No.	Task	Notes	✔
		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 71.		
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 71		
16	Configure the System Platform passwords. See Configuring System Platform passwords on page 72.		
17	Verify that System Platform installed correctly. See Verifying installation of on page 75.		
18	Check for System Platform patches and feature packs at http://support.avaya.com. Install any patches or feature packs that are available. See Installing patches on page 45 and Feature Pack installation on page 119.		
19	If your NMS uses SNMP v2c, change the SNMP version that is supported on the Services virtual machine. See Configuring SNMP version support on the Services VM on page 129.	The Services VM supports SNMP v3.	
20	Configure the SAL gateway for remote access and alarming. See SAL Gateway on page 80.		
21	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	

Table continues…

No.	Task	Notes	✔
		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.	
22	Generate and download license files for the template that is installed.		
23	Create an authentication file on the Authentication File System (AFS) and install it.		
24	If applicable, configure System Platform High Availability. See Configuring locally redundant High Availability on page 102.		

Related links

Upgrading a System Platform server on page 121

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

Before connecting directly to the services port, disable the proxy servers in Microsoft Internet Explorer.

Procedure

1. Start Microsoft 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 re-enable 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

Before connecting 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 re-enable 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 starts 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 might display an incorrect Keyboard Type. This issue has no effect on the installation process.

a. Open the PuTTy program.
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 63.

Related links

Connecting to the server through the services port on page 76

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 63.

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 64.

   - 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 65.

Next steps

- Verify that the System Platform image copied correctly to the DVD. See Verifying the System Platform image on the DVD on page 64.

  OR

- Configure the network settings for System Domain (Domain-0). See Configuring network settings for System Domain (Domain-0) on page 65

Verifying the System Platform server hardware

Before you begin

- You are performing a new installation of the System Platform software.
- You have completed the task, Selecting the type of keyboard on page 63

About this task

After Selecting the type of keyboard on page 63, 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 continues transparently to the next phase, Verifying the System Platform image on the DVD on page 64. 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 64

Verifying the System Platform image on the DVD

About this task

Use this procedure to verify that the System Platform image 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 becomes corrupt, you must write a new DVD with the System Platform image. Before using the new DVD, ensure 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 65.

Related links

Writing the ISO image to DVD or CD on page 54

Configuring network settings for System Domain

Procedure

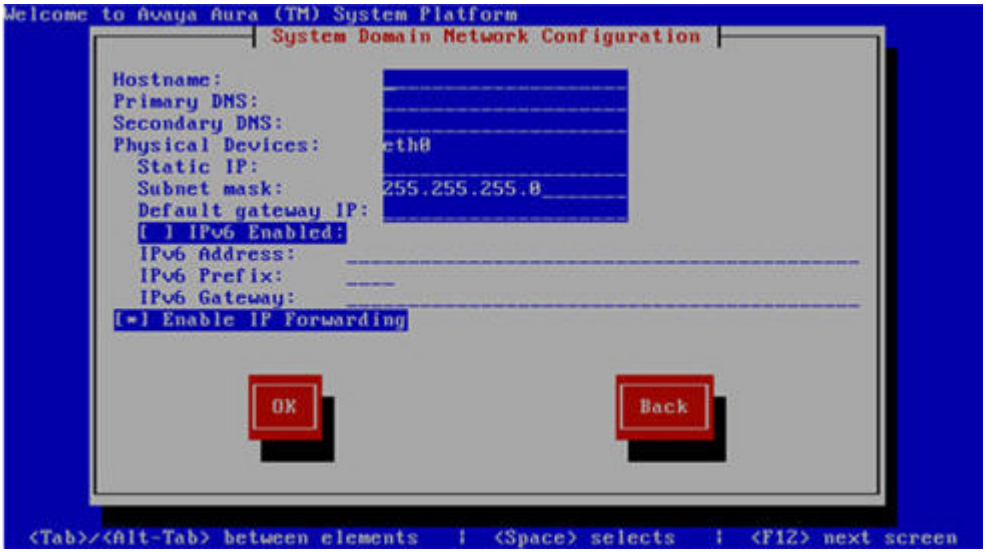
1. On the System Domain Network Configuration screen, complete the following fields:

   - **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 66.



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 displays. 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 67.

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.

Table continues…

Name	Description
Physical Devices	This field displays the physical Ethernet interface (NIC) that connects to the customer 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

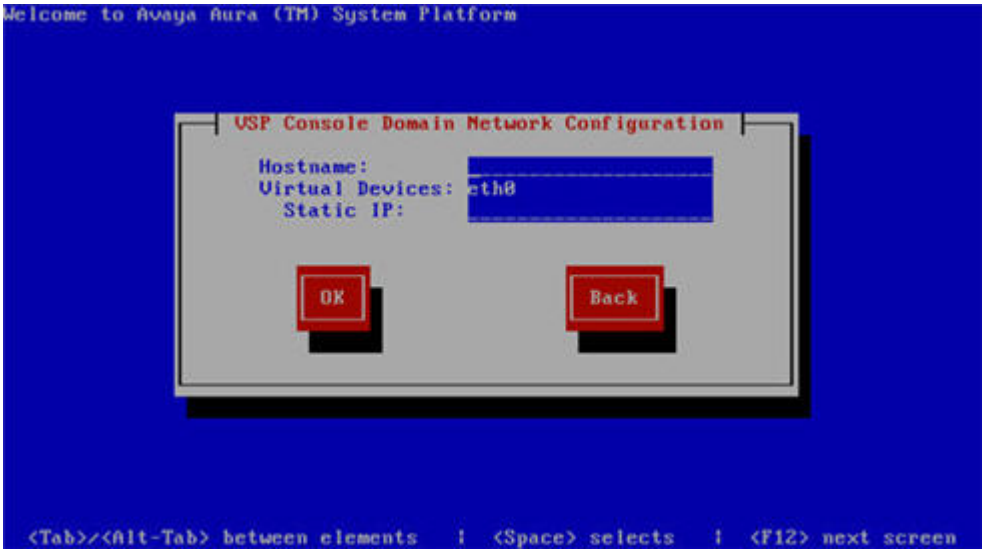
Procedure

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**



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 69.

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 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 earlier 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 can use Services VM 2.0, or you can upgrade your system to use a later version of the Services VM. When you upgrade the Services VM, the process preserves the earlier Master Agent configuration. For information on upgrading 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 displays 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 completed the task, “Configuring network settings for Console Domain.”
- If you plan to deploy a standalone 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 website at http://support.avaya.com.

About this task

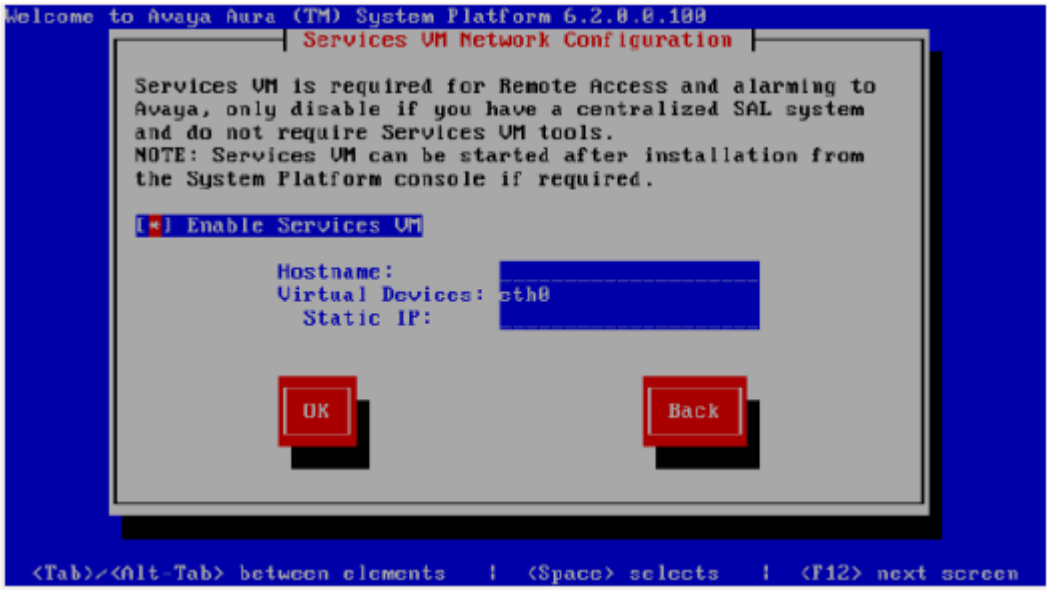
Use this procedure to install the Services VM in an enabled or disabled state, when the Services VM Network Configuration window displays during System Platform installation .

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 70.

   If you disable the **Enable Services VM** option, System Platform installation automatically continues 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.



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 links

Services VM Network Configuration field descriptions on page 71

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.

Related links

Installing the Services virtual machine on page 69

Configuring the time zone for the System Platform server

Procedure

1. On the Time Zone Selection screen, select the time zone of the server location.
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 on initial installation. Changing the time in a virtual machine environment causes virtual machines to restart.

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 secure. This account has a high-level of access to the system and steps must 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 by Avaya Services.

Procedure

1. You have the option of keeping the default passwords or changing the passwords.

   - If you want to change the passwords, complete steps 2 through 6 for each of the passwords.
   - If you do not enter new passwords, the defaults are used. Skip to step 7 to accept the default passwords.

   Important:

   Avaya recommends entering 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.

   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 The cust login is for audit purposes. It has read-only access to the Web Console, except for changes to its password, and no command line access.
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.

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. Click **User Administration** > **Change Password**.
3. Enter the old password in the **Old Password** field.
4. Type the new password.

   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.
5. Confirm the new password.

6. Click **Change Password**.
7. 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 postinstall scripts. After the installation is completed, the system ejects the DVD and restarts the server. If you are installing from server console, the system displays the Linux login page for System Domain (Domain-0) after the restart.

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 restart the server during the first boot process of Console Domain. If you shutdown or restart 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, try to go to the Web Console. See Accessing the Web Console on page 77.

Next steps

Verify System Platform installation. See Verifying installation of on page 75.

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. The cust login is for audit purposes. It has read-only access to the Web Console, except for changes to its password, and no command line access.
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

Table continues…

Name	Description
	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 access 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 77.

About this task

Important:

You cannot get 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 (Domain-0) command line as `root`, and run the **`check_install`** command.
- The Console Domain (Cdom) Web Console as `admin`.

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 help verify successful installation of System Platform . It can also identify various issues associated with an unsuccessful installation.

Important:

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

Procedure

1. Go to the System Domain command line.
2. Enter the command, **`check_install`**.

   If **`check_install`** finds no issues, the following message displays 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. Go to the System Platform Web Console.

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.

Related links

Accessing the command line for System Domain on page 78
Accessing the System Platform Web Console on page 77

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 links

Configuring the laptop for direct connection to the server on page 59
Disabling proxy servers in Mozilla Firefox on page 60
Disabling proxy servers in Microsoft Internet Explorer on page 60

Enabling IP forwarding to access System Platform through the services port

About this task

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

You can set the IP forwarding status to be enabled or disabled during System Platform installation. The system enables IP forwarding by default.

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 Domain-0 as administrator.
   c. In the command line, type **ip_forwarding enable**.
2. To disable IP forwarding:
   a. Start an SSH session.
   b. Log in to Domain-0 as administrator.
   c. In the command line, enter **ip_forwarding disable**.

      An alternative to the previous command is **service_port_access disable**.

Browser support for System Platform Web Console

The System PlatformWeb Console supports the following Web browsers:

- Microsoft Internet Explorer version 8 and version 9.
- Mozilla Firefox version 18 and version 19.

Accessing the System Platform Web Console

Before you begin

To access 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 77.

About this task

Important:

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

You can get to 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 Web browser on a computer that can route to the System Platform server.

   System Platform supports Microsoft Internet Explorer versions 7 through 9, and Firefox versions 3.6 through 19.

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 links

Enabling IP forwarding to access System Platform through the services port on page 77

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. You can also 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 use the command line for System Domain to perform a small number of tasks. Access to the command line for System Domain is reserved for Avaya or Avaya Partners for troubleshooting.

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 get the IP address of 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 get to Console Domain from System Domain, type **`xm list`**, note the ID for *udom*, and then type **`xm console`** *`udom-id`*. When prompted, log in 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 get to Console Domain until the system finishes the first boot process.

Note:

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

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 Platformincludes an embedded SAL Gateway.SAL Gateway software is also available separately for standalone deployments. The SAL Gateway program 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. The SAL gateway program 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 Internet connectivity to help 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 before 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.

Standalone SAL Gateway

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

If you use a standalone SAL Gateway, you must add it as an SNMP trap receiver for System Platform. See Adding an SNMP trap receiver on page 94. 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 94.

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 in the installed solution template. For example, virtual machines might include Communication Manager, Communication Manager Messaging, Session Manager, and other applications 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.

   Avayaassigns a Solution Element ID (SE ID) and Product ID to each SAL Gateway and managed device that is registered. In System Platform, managed devices are the components of System Platform and of the applications 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 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 links

Configuration prerequisites on page 81

Registering the system on page 51

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 *SAL Universal Install Form Help Document* form and submit the form to Avaya. The form includes complete instructions.

The SAL registration form is available at http://support.avaya.com. In the Help & Policies section, click **More Resources**. The system displays the More Resources page. Click **Avaya Equipment Registration**, and search for *SAL Universal Install Form Help Document*.

Note:

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

Related links

Registering the system on page 51
SAL Gateway on page 80
Registering the system on page 51

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 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 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:

- Microsoft Internet Explorer 7, 8, or 9
- Firefox 3.6 through 19

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 the 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.

   After you log in, the Managed Element page of the SAL Gateway user interface displays. If the SAL Gateway is 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 84.
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. 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 links

Gateway Configuration field descriptions on page 84

Applying configuration changes on page 91

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.
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

Table continues…

Name	Description
	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 links

Configuring the SAL Gateway on page 83
Registering the system on page 51

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) When 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 links

Proxy Server field descriptions on page 86
Applying configuration changes on page 91

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. **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.

Related links

Configuring a proxy server on page 85

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 defaults unless you are explicitly instructed to.

Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Core Server**.

   The Core Server page displays.

2. Do not change the defaults 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) When 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 links

Core Server field descriptions on page 87
Applying configuration changes on page 91

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.

Table continues…

Name	Description
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.

Related links

Configuring SAL Gateway communication with a Concentrator Core Server on page 87

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 defaults unless you are explicitly instructed to.

Procedure

1. In the navigation pane of the SAL Gateway user interface, click **Administration** > **Remote Server**.

   The Remote Server page displays.

2. Do not change the defaults on this page unless you are explicitly instructed to.
3. (Optional) When 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 closes all active connections.

Related links

Remote Server field descriptions on page 89
Applying configuration changes on page 91

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

Related links

Configuring SAL Gateway communication with a Concentrator Remote Server on page 88

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 links

Network Management Systems field descriptions on page 90
Applying configuration changes on page 91

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

Related links

Configuring NMS on page 89

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 displays several Gatew:ay Services such as:

   - **SAL Agent**
   - **Alarming**
   - **Inventory**
   - **Health Monitor**
   - **Remote Access**
   - **SAL Watchdog**
   - **SAL SNMP Sub-agent**
   - **Package Distribution**

   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 you stop the Remote Access service. Stopping the Remote Access service blocks 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, the System Domain 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 for 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	

Table continues…

Managed device (virtual machine)	IP Address	SE ID	Product ID	Model	Notes

Related links

Adding a managed element on page 92

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) 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 links

Managed Element field descriptions on page 93
Applying configuration changes on page 91
Managed element worksheet for SAL Gateway on page 91

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 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 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.

Table continues…

Name	Description
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.

Related links

Adding a managed element on page 92

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 standalone 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). See 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**.
   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 **Install**, and then, in the **Install Template From** field, select the location of the template 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 on page 99.
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 begin the template installation.

Note:

System Platform automatically performs a hardware check of the server platform. Servers supported by Avaya must meet all prerequisites for 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.

Note:

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 in the template. These pages vary according to the template you are installing. If you provided an EPW file, some of these pages 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 might 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) website. You must enter an Avaya SSO login and password. The list contains your company's templates. 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. **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 only displays if there is not an installed System Platform template.

Table continues…

Name	Description
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. Configures a proxy for Secure Access Link(SAL) and alarming functions to gain access to the Internet.
Upgrade	Upgrades the installed solution template from the selected template location option. This button only displays if there is an installed System Platform template.
Delete	Deletes the installed and active template. This button only displays if there is an installed System Platform template.

Configuring a proxy

About this task

If the template files are located on a different server (for example, Avaya PLDS or HTTP), configure a proxy server address and port.

Procedure

1. On the Search Local and Remote Template Patch page, click **Configure Proxy**.
2. On the System Configuration page, select **Enabled** for the **Proxy Status** field.
3. Specify the proxy address.
4. Specify the proxy port.
5. Click **Save** to save the settings and configure the proxy.

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 information about System Platform High Availability, see 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 the 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. When you finish template configuration, you can restart High Availability operation in the mode that you want

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 user name 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 uses System Platform FRHA, or MPHA with LMHA High Availability modes, you must satisfy all common prerequisites for all HA modes. You must also satisfy 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 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 crossover 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, usually 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 crossover 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. See the requirements of your specific solution template.
- Ensure that the default gateway replies to ICMP pings from each System Platform node. 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. It also contains 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 when 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 on 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 services_vm

Table continues…

VM Name	VM Description	Protection Mode
		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.
Crossover network interface	Network interface connected to the standby server. Required for internode 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.
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 might 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.

When 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 get to the Web Console on the standby server by using its IP address (provided during configuration of the High Availability feature).

Related links

Starting System Platform High Availability on page 107
Stopping System Platform High Availability on page 108

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.

Related links

High Availability start/stop on page 106

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 High Availability operation and returns System Platform to standard operation without High Availability protection. This procedure does not remove the High Availability configuration from either server.

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.

Related links

High Availability start/stop on page 106

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 many administrative, maintenance, or troubleshooting tasks affecting only one server. For example, use this procedure before replacing a hardware module on the active node in an Avaya Aura® system with High Availability protection.

Procedure

1. From the **Server Management** menu, click **High Availability**.
2. Click **Manual Interchange**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 before 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.

Upgrading System Platform

Preupgrade tasks

Preupgrade checklist

#	Task	Notes	✔
1	Download and install any patches for your current version of System Platform. See “Installing patches.”		
2	If you have not already done so, download all necessary System Platform upgrade files from DVD media, a USB storage device, or an HTTP server, or use File Manager to copy it to the target System Platform server's local `/vsp-template` directory.		
3	Check with your Avaya representative or the latest release notes for your solution template to confirm that it is compatible with the latest version of System Platform. If required, install recommended patches to your solution template to ensure compatibility with the version of System Platform that is qualified with your solution template.	You can download, install, and manage the regular updates and patches for solution templates at http://support.avaya.com. You can also download or install solution template patches from the Avaya Product Licensing and Delivery System (PLDS) at http://plds.avaya.com.	
4	Capture all current configuration settings from the **Server Managment** > **System Configuration** page of the Web Console.	You will need this information later to verify that all configuration settings carried forward during the upgrade process are correct and complete.	
5	Note the method of the date and time configuration that is set. Are the date and time manually set or configured to synchronize with an NTP server at a specific IP address?		
6	Back up System Platform and the solution template. See System Platform backup on page 113.		
7	If you are upgrading from System Platform 6.0, assign a new IP address to the Console Domain virtual machine and assign the former Console Domain IP address to the SAL Gateway. The	Perform this task only if you are upgrading from a System Platform version earlier than 6.2. If upgrading from System Platform 6.2 or later, this task is not required.	

Table continues…

#	Task	Notes	✔
	customer must provide to the installer one new IP address for Console Domain. See Cdom and SAL Gateway IP address assignments on page 114. **Note:** Perform this task only if the current version System Platform is using the embedded SAL Gateway. This task is not applicable if System Platform is currently using a stand-alone SAL Gateway.		

Preupgrade checklist for System Platform on High Availability systems

#	Task	Notes	✔
1	Download and install any patches for your current version of System Platform. See “Installing patches.”		
2	If you have not already done so, download all necessary System Platform upgrade files from DVD media, a USB storage device, or an HTTP server, or use File Manager to copy it to the target System Platform server's local `/vsp-template` directory.		
3	Check with your Avaya representative or the latest release notes for your solution template to confirm that it is compatible with the latest version of System Platform. If required, install recommended patches to your solution template to ensure compatibility with the version of System Platform that is qualified with your solution template.	You can download, install, and manage the regular updates and patches for solution templates at http://support.avaya.com. You can also download or install solution template patches from the Avaya Product Licensing and Delivery System (PLDS) at http://plds.avaya.com.	
4	Record all High Availability settings.		
5	Capture all current configuration settings from the **Server Managment** > **System Configuration** page of the Web Console.	You will need this information later to verify that all configuration settings carried forward during the upgrade process are correct and complete.	
6	Note the method of the date and time configuration that is set. Are the date and time manually set or configured to		

Table continues…

#	Task	Notes	✔
	synchronize with an NTP server at a specific IP address?		
7	Stop and remove High Availability on the primary server. See Stopping System Platform High Availability on page 108 and Removing the High Availability configuration on page 109.		
8	Back up System Platform and the solution template. See System Platform backup on page 113.		
9	If you are upgrading from System Platform 6.0, assign a new IP address to the Console Domain virtual machine and assign the former Console Domain IP address to the SAL Gateway. The customer must provide to the installer one new IP address for Console Domain. See Cdom and SAL Gateway IP address assignments on page 114. **Note:** Perform this task only if the current version System Platform is using the embedded SAL Gateway. This task is not applicable if System Platform is currently using a stand-alone SAL Gateway.	Perform this task only if you are upgrading from a System Platform version earlier than 6.2. If upgrading from System Platform 6.2 or later, this task is not required.	

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 High Availability operation and returns System Platform to standard operation without High Availability protection. This procedure does not remove the High Availability configuration from either server.

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.

Related links

High Availability start/stop on page 106

System Platform backup

With some exceptions, you can back up configuration information for System Platform and the solution template (all template virtual machines).

Note:

The System Platform backup feature does not back up the following types of configuration data:

- System parameters (examples: SNMP Discovery, Template product ID)
- Networking parameters (examples: Template IP and host name, Console Domain IP and host name, static IP route configuration)
- Ethernet parameters (examples: Auto-negotiation, speed and port information)
- Security configuration (examples: SSH keys, Enable Advance password, Host access list)

  In scenarios where, for example, an administrator performs a system backup prior to a template or platform upgrade or platform replacement, and the system generates new unique SSH keys internally as part of the upgrade or replacement action. The SSH keys generated prior to the backup operation are of no use to the system updated or replaced.

System Platform backs up sets of data and combines them into a larger backup archive. Backup sets are related data items available for backup. When you perform a back up, the system executes the operation for all backup sets. All backup sets must succeed to produce a backup archive. If any of the backup set fails, then the system removes the backup archive. The amount of data backed up depends on the specific solution template.

The system stores the backup data in the `/vspdata/backup` directory in Console Domain. This is a default location. During an upgrade, the system does not upgrade the `/vspdata` folder, facilitating a data restore operation if required. You can change this location and back up the System Platform backup archives to a different directory in System Platform or in an external server. Optionally, send the backup data to an external e-mail address if the file size is smaller than 10 MB.

If a backup fails, the system automatically redirects to the Backup page after login and displays the following message: `Last Backup Failed`. The system continues to display the message until a backup succeeds.

Important:

If you backup an instance of System Platform with not template installed, the server to which you restore the backup must also have no template installed. If any template is installed, the restore will fail.

Backups and restores across different versions of System Platform

You cannot restore an older version of System Platform from a backup created on a newer version of System Platform. For example, you cannot restore a System Platform 6.3 backup to System Platform 6.0. However, you can (for example), restore a System Platform 6.0 backup to System Platform 6.3, although not all templates support this ability. Confirm in your solution documentation

whether or not the solution template supports restoring an older version of System Platform backup to the current version.

Backups and System Platform High Availability

The System Platform backup feature does not provide a mechanism to reenable a failed System Platform High Availability node. For more information, see one of the following topics appropriate for your troubleshooting scenario:

- Re-enabling a failed preferred node to High Availability
- Re-enabling a failed standby node to High Availability

Utility Services settings and size of System Platform backups

Note:

This section applies only to templates that include Avaya Aura® Utility Services.

Avaya Aura® Utility Services has settings that control whether IP telephone firmware and Gateway firmware is included or excluded from all backups. These settings apply to backups performed in Utility Services or in System Platform.

- **Include Firmware in Backup**: Use this option to create a complete backup file, which includes IP telephone firmware and Gateway firmware. Backup files are very large and take longer to generate.
- **Exclude Firmware in Backup**: Use this option to create a backup file that excludes IP telephone firmware and Gateway firmware. Backup files are smaller and are much faster to generate.

For more information about the backup and restore in Utility Services, see *Accessing and Managing Avaya Aura® Utility Services*.

Cdom and SAL Gateway address assignments

Overview

If you are upgrading to System Platform 6.3 from a version earlier than 6.2, you must complete one of the following procedures. Choose the appropriate procedure depending on whether you are performing the upgrade from a remote location or on-site where the server is located:

- Reassigning Cdom and SAL Gateway IP addresses remotely on page 115
- Reassigning Cdom and SAL Gateway IP addresses onsite on page 117

Important:

Perform this task only if you are upgrading from a System Platform version earlier than 6.2. If upgrading from System Platform 6.2 or later, this task is not required.

Note:

This prerequisite does not apply to Avaya Aura solutions that have deployed a remote stand-alone SAL Gateway server. In this case, IP addresses assigned to your system must remain unchanged, because you will not enable the Services Virtual Machine during the platform upgrade process. During an upgrade, the System Platform installation software verifies if your system already uses the local SAL Gateway. If the system is not using the local SAL Gateway,

the System Platform installation program automatically installs the Services Virtual Machine in a disabled state, which also disables its embedded SAL Gateway.

On both procedures, you must assign a new IP address to the Cdom virtual machine, and then assign the former Cdom IP address to the SAL Gateway. The Avaya customer must provide any site-specific IP address assignments.

With System Platform versions 6.2 and later, a new Services Virtual Machine hosts the SAL Gateway unless you have already deployed a remote SAL Gateway server. You do not need to redefine alarm destinations for template applications running on the same server if you assigned both:

- The previous Cdom IP address to the embedded SAL Gateway and
- A new IP address to the Cdom virtual machine.

. You do not have to redefine alarm destinations because the IP address of the SAL Gateway remains unchanged throughout the upgrade process. Completing this process ensures that the SAL Gateway remains in communication with Avaya (or an Avaya Partner) during the upgrade event.

The following tables provide an example of Dom0, Cdom, and embedded SAL Gateway address assignments before and after completing the System Platform upgrade prerequisite:

Table 1: Example Dom0, Cdom, and SAL Gateway address allocations before upgrading to System Platform 6.3

Virtual Machine or Application	IP Address 1	IP Address 2
Domain 0 (dom0)	192.168.10.100	
Console Domain (cdom)		192.168.10.101 (shared)
Integrated SAL Gateway (version 1.8)		

Table 2: Example Dom0, Cdom, and SAL Gateway address allocations after upgrading to System Platform 6.3

Virtual Machine or Application	IP Address 1	IP Address 2	IP Address 3
Domain 0 (dom0)	192.168.10.100		
Console Domain (cdom)		(Reallocated to Services Virtual Machine.)	192.168.10.102 (New address assignment)
Integrated SAL Gateway (version 2.2) on Services Virtual Machine (services_vm)		192.168.10.101 (Reassigned from former cdom virtual machine)	

Reassigning Cdom and SAL Gateway IP addresses remotely

Perform this task when a System Platform upgrade must be performed from a location remote from the customer site. A Support Engineer at Avaya or an Avaya Partner site must complete this task entirely by communication established between an Avaya Remote Server and the server you must upgrade.

Before you begin

- If you are a customer of Avaya or an Avaya Partner and must upgrade to System Platform version 6.3 from a version earlier than 6.2, go tohttp://support.avaya.com and click on **Support Contact Options** > **Maintenance Support**.
- Complete the blank fields in the following table. The following steps reference either address “A” or “B”, as appropriate.

  Table 3: Cdom IP address assignments (remote procedure)

Current Cdom (avpublic) IP Address:	A.
New customer-provided IP address for Cdom: (The new address for the cdom virtual machine must be on the same IP subnet used by the System Platform Domain 0 virtual machine. Verify using Linux `ipcalc` or similar tool.)	B.

- Support Engineers must have their Token (SecureID) USB device available for additional authentication.

About this task

Important:

If you are upgrading a System Platform High Availability configuration that uses the embedded SAL Gateway, complete Cdom and SAL Gateway IP address reassignments on the primary server only, and only after stopping High Availability. If you later have a High Availability failover event (triggered manually or automatically), the High Availability subsystem enables the Services VM on the standby server. The HA data replication software also automatically propagates the new Cdom and SAL Gateway IP addresses to the standby server.

Use of the term *target server* in this procedure refers to the System Platform server you must upgrade.

Procedure

1. Log on to the SAL Remote Server at https://tech1.sal.avaya.com
2. Using the SE ID of VSPU (cdom), open a remote HTTPS SAL session with the Cdom virtual machine on the target server.
3. Log on to the System Platform Web Console, and log in as **admin**.
4. Click**Server Management** > **Network Configuration**.
5. From the **Domain Network Interface** panel, under the **Console Domain**, note the **avpublic** IP address from Table 3: Cdom IP address assignments (remote procedure) on page 116, field “A”.
6. Enter the new, customer-provided cdom IP address (from Table 3: Cdom IP address assignments (remote procedure) on page 116, field ”B”) into the Console Domain **avpublic IP** field.
7. Click **Save**.

Saving the change you made to the Cdom IP address configuration temporarily severs your secure connection to the target server. However, the server continues to have connectivity and communication with the remote Avaya servers. (Your SAL Gateway 1.8 gracefully manages changes to the server's IP address configuration.)

8. From the SAL Remote Server at https://tech1.sal.avaya.com, request an HTTPS session with the SAL Gateway on the target server.
9. Log on to the SAL Gateway user interface using the VSALGW SE ID: (https://<*localhost*>:7443)
10. Ypdate the Cdom managed element (VSPU) to match the value in Table 3: Cdom IP address assignments (remote procedure) on page 116, field “B”.
11. Click **Apply** and submit your changes to restart SAL Gateway services.
12. Disconnect from the SAL Gateway on the target server.
13. From the SAL Remote Server at https://tech1.sal.avaya.com, again request an HTTPS session with the Cdom virtual machine on the target server.

    This tunnel session now ends at the new address assigned to the Cdom virtual machine on the target server.
14. Using the SE ID of VSPU (Cdom), open a remote HTTPS SAL session with the Cdom virtual machine on the target server.
15. Log on to the Web Console of the target server.

Reassigning Cdom and SAL Gateway IP addresses onsite

Perform this task when a System Platform upgrade can be performed at the customer site. In this case, Avaya or Avaya Partner Support Engineering personnel are available onsite to assist with local (customer network) login to the Web Console for the server that you must upgrade.

Before you begin

- If you are a customer of Avaya or an Avaya Partner and must upgrade to System Platform version 6.3 from a version earlier than 6.2, go tohttp://support.avaya.com and click on **Support Contact Options** > **Maintenance Support**.
- Complete the blank fields in the following table. The following steps reference either address “A” or “B”, as appropriate.

Table 4: Cdom IP address assignments (local procedure)

Current Cdom (avpublic) IP Address:	A.
New customer-provided IP address for Cdom: (The new address for the cdom virtual machine must be on the same IP subnet used by the System Platform Domain 0 virtual machine. Verify using Linux `ipcalc` or similar tool.)	B.

- Support Engineers must have their Token (SecureID) USB device available for additional authentication.

About this task

Important:

If you are upgrading a System Platform High Availability configuration that uses the embedded SAL Gateway, complete Cdom and SAL Gateway IP address reassignments on the primary server only, and only after stopping High Availability. If you later have a High Availability failover event (triggered manually or automatically), the High Availability subsystem enables the Services VM on the standby server. The HA data replication software also automatically propagates the new Cdom and SAL Gateway IP addresses to the standby server.

Procedure

1. Log on to the System Platform Web Console as `admin`.
2. Select **Server Management** > **Network Configuration**.
3. From the **Domain Network Interface** panel, under the **Console Domain**, note the **avpublic** IP address in preceding table, field “A”.
4. Enter the new, customer-provided Cdom IP address (from the preceding table, field ”B”) into the Console Domain **avpublic IP** field.
5. Click **Save**.

   Saving the change you made to the Cdom IP address configuration temporarily severs your secure connection to Cdom on the target server. However, the server continues to have connectivity and communication with the remote Avaya servers. (Your SAL Gateway 1.8 gracefully manages changes to the server's IP address configuration.)
6. Log on to the SAL Gateway user interface using the new Cdom IP address (https://*<new_Cdom_IP>*:7443) and update the Cdom managed element (VSPU) to match the value in the preceding table, field “B”.
7. Log on to the System Platform Web Console as `admin` and check for errors.
8. Select **Server Management** > **Network Configuration**.
9. Verify that the Web Console displays the new Cdom IP address in the Console Domain **avpublic IP** field.

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, so always see your solution documentation for specific prerequisites and installation instructions.

Guidelines for RPM-based feature packs

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

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

Guidelines for ISO-based feature packs

For any ISO-based System Platformfeature pack, 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 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 configuration.

Feature Pack installation

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

RPM-based feature packs

For RPM-based feature packs (for example, Feature Pack 3, System Platform 6.3.4), see Patch management on page 43.

ISO-based feature packs

For ISO-based feature packs (for example, Feature Pack 2, System Platform 6.3), perform a platform upgrade.

Platform upgrade process in different System Platform deployments

This topic provides a summary of different System Platform deployments and, for each deployment, the platform upgrade process.

Deployment scenarios for the System Platform upgrade process are as follows:

- Simplex (single-server) deployment
- SAL Gateway configuration prior to System Platform upgrade:
  - Embedded SAL Gateway
  - Standalone SAL Gateway
- Primary server upgrade for System Platform HA
- Secondary (standby) server upgrade for System Platform HA
- Services Virtual Machine installed state after dual-server upgrade for System Platform HA

The following table summarizes deployment options and the outcomes to expect during and after a System Platform upgrade:

Table 5: System Platform deployments and upgrade outcomes

Server upgrade type	SAL Gateway type	Cdom and SAL Gateway address reassignment	Services Virtual Machine installed state after upgrade
Simplex (single-server)	Embedded gateway	Yes	Enabled, to support embedded SAL Gateway operation.
Simplex (single-server)	Standalone gateway	No, but an IP address must be reserved for the location of the standalone gateway.	Disabled, since no requirement exists for operation of the SAL Gateway on the Services Virtual Machine.
Duplex (dual-server) for System Platform High Availability: *Primary server*	Embedded gateway	Yes	Enabled to support embedded SAL Gateway operation after platform upgrade.
Duplex (dual-server) upgrade for System Platform High Availability: *Primary server*	Standalone gateway	No, but an IP address must be reserved for the location of the standalone gateway.	Disabled, since no requirement exists for operation of the SAL Gateway on the Services Virtual Machine.
Duplex (dual-server) upgrade for System	Embedded gateway, but no System Platform HA	No. System Platform HA software activates the	Disabled until automatic or manual failover, when

Table continues…

Server upgrade type	SAL Gateway type	Cdom and SAL Gateway address reassignment	Services Virtual Machine installed state after upgrade
Platform High Availability support: *Secondary (standby) server*	configuration required on the secondary/standby server.	Services VM on the standby server and propagates the HA configuration (including use of the embedded SAL Gateway) to that server on automatic or manual failover.	the Services Virtual Machine must support operation of the embedded SAL Gateway on the Services Virtual Machine.
Duplex (dual-server) upgrade for System Platform High Availability support: *Secondary (standby) server*	Standalone gateway, but no System Platform HA configuration required on the secondary/standby server.	No. System Platform HA data replication software automatically propagates the HA configuration (including use of the standalone SAL Gateway configuration) to the standby server on automatic or manual failover.	Remains disabled after automatic or manual failover, since no requirement exists for operation of the embedded SAL Gateway on the Services Virtual Machine.

Upgrading a System Platform server

This is a procedure for performing a full platform upgrade on your System Platform server, from an earlier version to a later version of the System Platform software. You can also use this procedure to install new feature pack software offered only in ISO format, since this scenario also follows the full platform upgrade process. Use standard patch management procedures to install any feature pack software offered only in RPM (patch) format.

Before you begin

- Perform all preupgrade tasks that are listed in Preupgrade checklist on page 110.
- If you are upgrading two servers supporting a System Platform High Availability configuration, **Stop HA** and then **Remove HA** on the Primary server. System Platform does not support platform upgrades while High Availability is running. If you attempt an upgrade while High Availability is running, a warning message appears and the system prevents you from performing the upgrade.

Procedure

1. Log in to the Web Console for the primary (if HA) or standalone (if non-HA) System Platform server.
2. Click **Server Management** > **Platform Upgrade** in the navigation pane.

   The Server Management Platform Upgrade page appears.
3. In the **Upgrade Platform From** field, select the location of the software to be installed.

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 on page 99.

4. If you selected **HTTP** or **SP Server** in the **Upgrade Platform From** field, enter the complete URL or path of the platform upgrade files.
5. Click **Search**.

   The system searches the location that you specified for an upgrade description file that has an .ovf extension.
6. Select the VSP description file for the platform upgrade, and then click **Select**.

   The system displays the version and additional information for the current and the new platform on the Platform Upgrade Details page.
7. On the Platform Upgrade Details page, click **Upgrade**.

   Important:

   As part of the upgrade process, the System Domain (Domain-0) and Console Domain virtual machines will reboot.
8. Click **OK** when prompted to confirm that the template has been qualified for the platform version to which you are upgrading, and that both the System Platform Web Console and Console Domain will reboot upon completion of the upgrade .
9. Click **OK** when prompted to confirm the upgrade.

   At this stage, the upgrade process starts and the system displays the Platform Upgrade workflow status page.

   Note:

   The System Domain (Domain-0) and Console Domain reboot at this stage. For this reason, the Platform Upgrade workflow status page does not show any updates until it reboots in the new Console Domain. After the Web Console is up, the system automatically redirects you to the login page. This routine can take approximately 20 minutes.
10. Log in to the System Platform Web Console.

    Note:

    You are allowed a 4-hour period to log in to the System Platform Web Console. If you do not login during this period, the system will reboot using the previous release of System Platform. If a user logs in to System Platform Web Console within the 4-hour period, it is assumed that System Platform is reachable and the timer is cancelled.
11. Before electing to commit or roll back the platform upgrade, complete the procedure for verifying an upgrade.

12. On the Commit or Rollback platform upgrade page, perform the procedure to either commit the upgrade or rollback the upgrade.
13. If you elected to commit the upgrade and the system finishes rebooting automatically, log on to the upgraded server's Web Console.
14. Select **SAL Gateway Management**.

    Note:

    If your network includes a standalone SAL gateway, the platform upgrade leaves the embedded SAL Gateway disabled on the local Services Virtual Machine. You must administratively configure the details of the standalone server and then enable the SAL gateway to run on that server.
15. Click **Enable SAL Gateway**.
16. Click **Launch SAL Gateway Management Portal**.

    The Avaya SAL Gateway user interface appears.
17. Log on to the SAL Gateway user interface.

    The default username is `admin`; the default password is `admin01`.
18. Click **Administration** > **Service Control & Status**.

    The Gateway Service Control window opens.
19. Click **Check Health for the Gateway** on the Gateway Service Control page.

    This action displays results of a final check for proper SAL Gateway operation and communication with Avaya remote servers.

    This completes the System Platform upgrade procedure.

Related links

Installation checklist for System Platform on page 55

Configuring a proxy

About this task

If the template files are located on a different server (for example, Avaya PLDS or HTTP), configure a proxy server address and port.

Procedure

1. On the Search Local and Remote Template Patch page, click **Configure Proxy**.
2. On the System Configuration page, select **Enabled** for the **Proxy Status** field.
3. Specify the proxy address.
4. Specify the proxy port.
5. Click **Save** to save the settings and configure the proxy.

Commit and Rollback

System Platform upgrades must be committed before performing other operations, including installation of patches. During an upgrade, after the system boots in the new platform release, the user is required to commit or rollback the upgrade. While the system is waiting for the user to either commit or rollback, Avaya advises not to perform any of the following operations:

- Delete a template
- Install a template
- Upgrade a template
- Reboot the System Platform Web Console

  Note:

  Rebooting System Platform Web Console before committing will roll back the system to the previous release.
- Install or remove a patch
- Start High Availability operation

Commit

You can commit an upgrade when you are satisfied that the new System Platform software is working without any issues. After committing an upgrade, you cannot go back to the older version of the System Platform software. If you do not log in to System Platform Web Console within 4 hours after the upgrade, the system performs an automatic rollback.

The system performs the following when you commit an upgrade:

- Performs a clean up operation (such as, removing state files and so on).
- Commits boot loader (grub) to boot up into the new platform from now on.
- Marks the Workflow as complete and indicates that on the Platform Upgrade Status page.

Rollback

You can perform a rollback operation if you find any errors or issues with the new System Platform software and must go back to the older version of software. Rollback reboots the server.

The system performs the following when you roll back an upgrade:

- Performs a clean up operation (such as, removing state files and so on).
- Prepares the system to notify the user of the reason for rollback after rebooting into the old platform.
- Reboots the platform to boot up into the old platform and restores access to System Platform Web Console.

Committing an upgrade

Procedure

On the Commit or Rollback platform upgrade page, click **Commit** to continue the platform upgrade process.

Rolling back an upgrade

Procedure

On the Commit or Rollback platform upgrade page, click **Rollback** to cancel the upgrade process and go back to the previous version of the software.

Note:

After a rollback, when you log on to the System Platform Web Console, the system displays the Rollback Acknowledge page that specifies the reason for rollback (either user initiated rollback or deadmans switch) based Auto rollback; or if the upgrade failed and the system rebooted to an older version of System Platform as part of fail-safe fallback mechanism.

Verifying an upgrade

Before you begin

You have performed all of the platform upgrade steps leading up to, but not including, the commit or rollback step. Before returning to commit or rollback and then finishing the procedure for Upgrading a System Platform server on page 121, you must first complete all of the checks in the following procedure successfully.

About this task

This procedure helps to verify certain key indications of a successful platform upgrade, for example:

- the new System Platform version running on the server
- the presence and versions of virtual machines required for your Avaya Aura® solution
- networking and user configuration capabilities
- Network Time Protocol (NTP) configuration

Procedure

1. Log on to the Web Console as **admin**.

   You should see the **Commit/Rollback** page, which verifies:

   - The server successfully booted up to the new platform version.
   - No image or kernel faults occurred during the upgrade. Otherwise, System Platform automatically rolls back into its prior version and the **Rollback Acknowledge** page appears.

- No problems occurred in LDAP storage.

2. Go to **Server Management** > **System Configuration** in the Web Console and verify that all the system configuration information is accurate before committing the upgrade.

   This action performs a quick check for accuracy of system configuration information carried forward during the platform upgrade.

3. On the **Virtual Machine Management** page, verify that the Domain-0 and Console Domain (cdom) versions are identical to the version of your System Platform upgrade (6.3 or later).

4. Use SSH to log on to Dom-0 and Cdom as an advanced administrator (**admin**) and run the `swversion` command.

   The command output should verify the new System Platform version (6.3 or later).

5. If an administrator installed a solution template before performing the System Platform upgrade, use the Web Console to verify that all virtual machines for the installed template are visible and accessible. (Click on the virtual machine links and verify their version labels.)

6. Go to **Server Management** > **Date/Time Configuration** in the Web Console and verify that the Date and time are correct as configured prior to the upgrade (manual date/time setting or configured to synchronize with an NTP server at a specific IP address).

   This action performs a quick sanity check on the NTP protocol, date, and time configuration.

7. Go to **Server Management** > **Backup/Restore** > **Restore** in the Web Console and note the latest backup information.

   A successful backup during platform upgrade should result in a file visible at this location. As such, this action performs a quick sanity check on System Platform backup/restore functionality.

8. Go to **Server Management** > **Network Configuration** in the Web Console and verify that all network configuration values are correct as configured.

   This action performs a quick validation of the System Platform networking setup.

9. If possible at this time, go to **User Administration** > **Local Management** in the Web Console, and then click **Create User** to create a test user.

10. **Delete** the test user.

    The last two steps together perform a quick check for user administration functionality.

11. Go to **Server Management** > **SAL Gateway Management** in the Web Console.

    If you chose **Enable Services VM** during the platform upgrade procedure, the SAL Gateway should be running. Otherwise (if you deploy the SAL Gateway on a separate stand alone server), the embedded SAL Gateway should be stopped. This action verifies availability of the SAL Gateway running on the Services Virtual Machine.

12. Go to **Server Management** > **SNMP Trap Receiver Configuration** in the Web Console and verify that all the SNMP trap receivers configured before the platform upgrade have been carried forward into the new version of System Platform.

The upgrade process automatically adds a trap receiver of 127.0.0.1 if the Services Virtual Machine is, by default, still enabled. Otherwise, you must add trap receiver destinations corresponding to Network Management Systems in your own network, including one for an external SAL Gateway.

13. Trigger a test alarm from the Cdom Command Line Interface (CLI) and verify that all configured SNMP trap receivers did receive the alarm.

    The last two steps together perform a quick check for SNMP trap receiver functionality.

14. Go to **Server Management** > **License Management** in the Web Console and launch the **WebLM License Manager**.
15. Log in to WebLM portal to verify that all template virtual machine license files are still valid.

    The last two steps together perform a quick check on WebLM functionality in the new version of System Platform.

16. Return to step 12 on page 123 of Upgrading a System Platform server on page 121

Platform Upgrade field descriptions

Name	Description
Upgrade Platform From	Lets you specify the location from where to download or upload the template image files for the platform upgrade. Options are: • **Avaya Downloads (PLDS)** The files are located in the Avaya Product Licensing and Delivery System (PLDS) Web site. You must enter an Avaya SSO login and password. • **HTTP** The files are located on an HTTP server. You must specify the URL of the platform upgrade if you select this option. • **SP Server** The platform upgrade files are located in the `/vsp-template` directory in the System Platform Console Domain. You must copy the platform upgrade files in this directory using a file transfer program and change their permissions as follows: `chmod 644 <files-copied>` • **SP CD/DVD** The files are located in a CD or DVD.

Table continues…

Name	Description
	• **SP USB Device** The files are located on a USB flash drive. This option is: - supported for RPM patch upgrades not exceeding the storage capacity of the flash drive. - not supported for full-platform (ISO) upgrades to System Platform 6.2 or later.
SSO Login	Single Sign-On username required when the **Upgrade Platform From** source is **Avaya Downloads (PLDS)**.
SSO Password	Single Sign-On password required when the **Upgrade Platform From** source is **Avaya Downloads (PLDS)**.
Platform Upgrade URL	URL required when the **Upgrade Platform From** source is either **HTTP** or **SP Server**.

Button descriptions

Button	Description
Search	Searches for a template description file that has an .ovf (Open Virtualization Format) extension at the location that you specify. Opens the Platform Upgrade Details page with the search results. **Note:** Open virtualization format (OVF) is an open standard for packaging and distributing software that runs on virtual machines.
Configure Proxy	Redirects to the System Configuration page after clicking **Search**, enabling you to configure a proxy server (if needed) to reach the **Avaya Downloads (PLDS)** server, an **HTTP** server, or a System Platform server (**SP Server**) chosen as the source for platform upgrade file downloads.
Select	Selects the template description file you require to upgrade your system. (You identified the file after searching your upgrade file source: (PLDS, HTTP, or SP Server).
Upgrade	Upgrades the system with the template description file you selected after searching your upgrade file source (PLDS, HTTP, or SP Server).

Table continues…

Button	Description
Commit	Commits an upgrade operation and upgrades the System Platform software to the latest version. **Note:** After executing a commit operation, you cannot go back to the older version of the System Platform software. If you do not execute a commit operation within 4 hours after the upgrade, the system performs an automatic rollback.
Rollback	Cancels an upgrade operation, and the system goes back to the previous version of System Platform software.
Acknowledge	Lets you confirm the reason for the rollback operation.

Postupgrade tasks

Configuring SNMP version support on the Services VM

Before you begin

You must have:

- Root level access to the Linux command line on the Services virtual machine
- The default community string for SNMPv2c: avaya123
- The default user string for SNMPv3: initial
- The SNMPv3 password: avaya123

After successfully configuring SNMP version support on the System Platform server, use the SNMP community, user, and password strings to perform services-specific operations (for example, SNMP querying) on the Services VM.

About this task

Use the following steps to change the Net-SNMP Master Agent configuration on the Services virtual machine. You change the Master Agent configuration to match the version of SNMP (v2c or v3) required by your NMS.

For upgrades to System Platform 6.3, this task is required only if you are upgrading from System Platform 6.0.3. If you are upgrading from System Platform 6.2 or later, the existing Net-SNMP Master Agent configuration is preserved.

Procedure

1. Open an SSH session to log on to the Services VM as **root**.
2. Change the current directory to `/etc/snmp`.
3. Find the **snmpd.conf** file.

4. Check the version of **snmp<v2c| v3>.conf** linked to the file **snmpd.conf** .

   For example:

   # ls –l

   ```
   lrwxrwxrwx 1 root root 11 Jul 19 20:35 snmpd.conf -> snmpv3.conf
   -rw-r--r-- 1 root root 77 Jun 28 11:54 snmpv2c.conf
   -rw-r--r-- 1 root root 72 Jun 28 11:54 snmpv3.conf
   ```

5. If the **snmpd** service is active, run the following command to stop the service:

   /sbin/service snmpd stop

6. Run the following command to back up the file **snmpd.conf** :

   cp snmpd.conf snmpd.conf.bak

7. Run the following command to remove **snmpd.conf**:

   rm –f snmpd.conf

8. Run one of the following commands to create a soft link to the SNMP version you want to support:

   To configure the Master Agent for SNMP v3:

   ln –s snmpv3.conf snmpd.conf

   To configure the Master Agent for SNMP v2c:

   ln –s snmpv2c.conf snmpd.conf

9. Run the following command to start the **snmpd** service:

   /sbin/service snmpd start

Upgrading the Services virtual machine

Before you begin

- Do not attempt to upgrade the Services virtual machine until you have completed the upgrade process to System Platform 6.3 and committed the upgrade.
- Download the upgrade to Services VM 2.0.
- On High Availability systems:
  - From the primary server, **STOP HA**.
  - After stopping High Availability, **REMOVE HA** from the primary server.

About this task

If you are upgrading from System Platform 6.2.x, use this procedure to upgrade the Services virtual machine to version 2.0. If you are upgrading from System Platform 6.0.3, this procedure is not required. Services VM version 2.0 is included in your upgrade to System Platform 6.3.

You must log in to the Web Console within four hours of the upgrade. If you do not, the Services virtual machine rolls back to the previous version.

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

   The system displays the Search Local and Remote Template page.
5. Next to `Services_VM`, click **Upgrade**, and then, in the **Install Template From** field, select the location of the software to be installed.

   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 on page 99.
6. If you selected **HTTP** or **SP Server** in the **Install Template From** field, enter the complete URL or path of the template files.
7. Click **Search**.
8. Select the **Services_VM** template, and then click **Select** to continue.
9. On the Template Details page, click **Install**.
10. On the Template Network Configuration page, confirm the network settings, and then click **Save**.
11. On the Template Details page, click **Install**.

    The Template Installation page displays the progress of the upgrade.
12. If your system is a High Availability system, perform the following steps:
    a. Navigate to the High Availability page.
    b. From the primary server, click **Configure HA**, and then reenter your System Platform High Availability configuration.
    c. Click **Create** to save the HA configuration.
    d. From the primary server, **START HA**.

Next steps

Confirm that SAL Gateway is running.

Upgrading Services-VM on System Platform

Services-VM 3.0 supports direct upgrade from versions 1.0.x and 2.0.

After System Platform installs Services-VM for the first time, you must maintain Services-VM in the same way as a solution template. Services-VM follows the same methods for announcements, distribution, and installation of a solution template. You must apply the Services-VM upgrades only through the System Platform Web Console, in the same way as for all other solution templates.

Caution:

Never directly upgrade Avaya Diagnostic Server and the components that are running on Services-VM. You must upgrade Avaya Diagnostic Server and the components on Services-VM only through the Services-VM upgrade process.

Important:

You must perform backup and restore operations of the Avaya Diagnostic Server components, such as SAL Gateway, on Services-VM through the integrated Backup and Restore features on the System Platform Web Console. The Services-VM upgrade process does not save the backup archives that you create locally on Services-VM by using the backup features of Avaya Diagnostic Server components.

About this task

The Services-VM upgrade procedure is similar to the upgrade procedure of other solution templates on System Platform. This section mainly describes the steps that you must do differently for Services-VM from a template upgrade. For more information about upgrading a solution template, see *Upgrading Avaya Aura® System Platform*.

Procedure

1. Log on to the System Platform Web Console as an administrator.
2. If you have an ISO image for the Services_VM upgrade, write the ISO image to a DVD, and insert the DVD in the System Platform server CD-ROM or DVD drive.

   Important:

   The preferred method for upgrading Services-VM is to write the ISO image to a DVD and then choosing the **CD/DVD** option to install the template.
3. If you have an ISO image but do not have physical access to the server, perform the following steps.

   Important:

   You must perform the following steps as the root user. Perform all operations carefully. The incorrect use of the root account might affect the performance of the system.

   a. Transfer the Services-VM image file to the cdom virtual machine as the admin user.

      You can use the **scp** command to copy the file from a Linux system to the remote virtual machine. To copy the file from a Windows system, you can use WinSCP or a similar file transfer tool.

   b. Establish an SSH session to cdom as the root user.

   c. Create the mount directory for the image file of Services-VM.

      For example:

      ```
      mkdir /mnt/Services_VM
      ```

   d. Change the directory to the location where you copied the image file.

   e. Mount the image file on the mount directory that you created earlier.

For example:

```
mount -o loop Services_VM-3.0.0.0.X.iso /mnt/Services_VM
```

f. Copy the folder where you mounted the ISO image to the `/vsp-template` folder.

For example:

```
cp -r /mnt/Services_VM /vsp-template/
```

g. List the files in the `/vsp-template/Services_VM` folder to check that the copy operation is successful.

The following is a sample output of the **ls** command for the `/vsp-template/Services_VM/` folder:

```
ls -l /vsp-template/Services_VM/
```

```
total 839000
-r-------- 1 tomcat tomcat      5811 Aug 27 18:20 backup_sdom.sh
-r-------- 1 tomcat tomcat      2507 Aug 27 18:20 index.html
-r-------- 1 tomcat tomcat     12090 Aug 27 18:20 patch_sdom.sh
-r-------- 1 tomcat tomcat      4084 Aug 27 18:20 resizeVM.sh
-r-------- 1 tomcat tomcat 858218207 Aug 27 18:21 services_vm.gz
-r-------- 1 tomcat tomcat     12316 Aug 27 18:21 Services_VM_Medium.ovf
-r-------- 1 tomcat tomcat       522 Aug 27 18:21 Services_VM.mf
-r-------- 1 tomcat tomcat     12270 Aug 27 18:21 Services_VM_Small.ovf
-r-------- 1 tomcat tomcat      4448 Aug 27 18:21 srvcs-vm-srvc-control.sh
-r-------- 1 tomcat tomcat      2673 Aug 27 18:21 versioninfo_sdom.sh
```

h. Unmount the image file.

For example:

```
umount /mnt/Services_VM
```

i. Remove the folder that you created for mounting the ISO image.

For example:

```
rm -rf /mnt/Services_VM
```

4. In the left navigation pane of the System Platform Web Console, click **Virtual Machine Management** > **Templates**.

The Search Local and Remote Template page displays the Services-VM version and the solutions templates installed on System Platform.

5. Click **Upgrade** next to the Services-VM version installed.

6. In the **Install Template From** field, select the location from where the system must install the Services-VM upgrade. Follow the same steps as you do to search and select a template for upgrade in System Platform.

If you copied the ISO image file for Services-VM to the server, select **SP Server**.

If you wrote the ISO image to a DVD and inserted the DVD to the server CD or DVD drive, select **SP CD/DVD**.

7. Select the appropriate Open Virtualization Format (OVF) file for Services-VM according to your common release server.

The following table lists the OVF file that you must select depending on the common server release.

Common server release	OVF file
R1	`Services_VM_Small.ovf`
R2	`Services_VM_Medium.ovf`

The Template Details page displays the version and additional information about the current and the new template for Services-VM.

8. Select the check box next to the **Normal** configuration, and click **Install**.

   The Template Network Configuration page displays the general network settings for Services-VM.

9. Click **Save**.

   The Template Details page displays the default values for Services-VM.

10. If required, change the default values.

11. Click **Install**.

    The upgrade process starts and the Template Installation page displays the progress of the upgrade process.

    Note:

    As part of the upgrade process, the system stops Services-VM at this stage, which results in termination of the SAL Gateway services running on Services-VM. The temporary termination of the services causes termination of all established connections to SAL Gateway and might result in product alarms being missed. If you have connected to the System Platform Web Console remotely through the SAL Gateway that is on board, the system logs you off from the Web Console at this stage. The Services-VM upgrade process continues in the background until all tasks in the upgrade process are complete.

    Note:

    The first task in the process, downloading the disk image for Services-VM, might take varied amount of time to complete. The completion time depends on the location of the server from which you download the template and the network quality, such as bandwidth and traffic. The other tasks take approximately 20 minutes to complete.

12. Log on to the System Platform Web Console to check the progress of the upgrade process.

    After the completion of the upgrade tasks, the Template Installation page displays two buttons, **Commit Installation** and **Rollback Installation**.

13. Verify the upgrade, and perform one of the following actions:

    - Click **Commit Installation** to apply the newly upgraded Services-VM.
    - Click **Rollback Installation** to cancel the upgrade process and return to the previous version of Services-VM.

Important:

You must log on to the Web Console within *4 hours* of the completion of the upgrade tasks and commit the upgrade process. Otherwise, the system cancels the upgrade process and automatically rolls back to the previous version of Services-VM.

Confirming that SAL Gateway is running

About this task

Use this procedure that confirm that SAL Gateway is running after an upgrade of the Services virtual machine.

Procedure

1. Select **Server Management** > **SAL Gateway Management** in the navigation pane of the System Platform Web Console.
2. On the SAL Gateway Management page, click **Enable SAL Gateway** if it is displayed.

   If **Disable SAL Gateway** is displayed, SAL Gateway is already enabled.
3. Click **Launch SAL Gateway Management Portal**.
4. Log on to the SAL Gateway user interface.

   The default username is `admin`; the default password is `admin01`.
5. Click **Administration** > **Service Control & Status**.

   The Gateway Service Control window opens.
6. Click **Check Health for the Gateway** on the Gateway Service Control page.

   This action displays results of a final check for proper operation of SAL Gateway and communication with Avaya remote servers.

Next steps

Commit the upgrade of Services VM.

Committing the template upgrade

Procedure

When the upgrade is complete, click **Commit Installation** on the Template Installation page. Or, to cancel the upgrade and revert to the previously installed software version, click **Rollback Installation**.

Installing the System Manager Release 6.3 template using ISO

Before you begin

- Disable the pop-up blocker for the web browser to continue with the installation.
- Download the `System_Manager_06_03_Version_II.iso` file that contains the System Manager installation files.

About this task

When you install System Manager on a virtual machine by using the System Manager template, the system installs the Linux operating system, CentOS, and the System Manager software. The installation process takes about 40–50 minutes to complete.

Procedure

1. Perform the following:
   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_Version_II.iso` file to the `/tmp` folder by using the software, such as WinSCP.
   d. At the command prompt, type `mount -o ro loop /tmp/System_Manager_06_03_Version_II.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`
      - `System_Manager_06_03_Version_II.tar`
      - `System_Manager_06_03_Post_Deploy.tar`
      - `SystemManager.mf`
      - `SystemManager.ovf`
2. To log on to the System Platform web console:
   a. In the web browser, type `https://<IPAddress of the C-dom web console>`.
   b. Use the administrator credentials made available at the time of the System Platform installation.
3. In the left navigation pane, click **Virtual Machine Management** > **Templates** > **Install**.
4. On the Search Local and Remote Template page, select an appropriate installation mode.

   Note:

   You can download the installation files from the Avaya Support website or extract the 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 about selecting a template, see Search Local and Remote Template field descriptions section in *Administering Avaya Aura® System Manager*.

5. To search the installation OVF file, click **Search**.
6. In the **Select Template** field, click the `SystemManager.ovf` file, and click **Select**.
7. On the Select Template page, click **Continue without EPW file** > **Upgrade**.

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

   This IP address must be different from the IP address of the C-dom and Dom-0 virtual machines.
9. 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 whitespace is before the first character or after the last character, the system removes the whitespace and proceeds with the installation.
10. In the **Domain** field, enter the domain name of the virtual machine.
11. Click **Next Step**.
12. On the VFQDN page, change the default values in the following field:
    a. **Virtual Hostname**: enter a unique host name.
    b. **Virtual Domain**: enter a unique domain name.

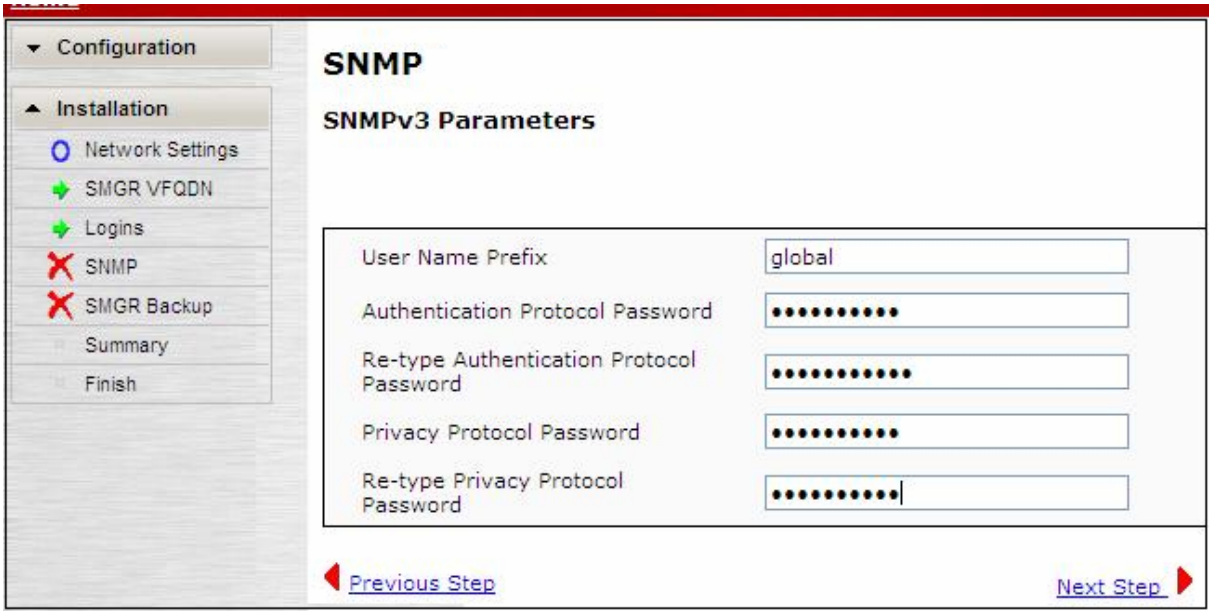
       Note:

       - The VFQDN value must be unique and different from the FQDN value of System Manager and the elements.
       - VFQDN is a mandatory field.
       - Do not add VFQDN entries in the DNS configuration.
       - Do not add VFQDN in the `/etc/hosts` file on System Manager. Adding VFQDN in the `/etc/hosts` file might cause failures.
       - In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN.
       - After the System Manager installation, you cannot change the VFQDN unless you reinstall System Manager.

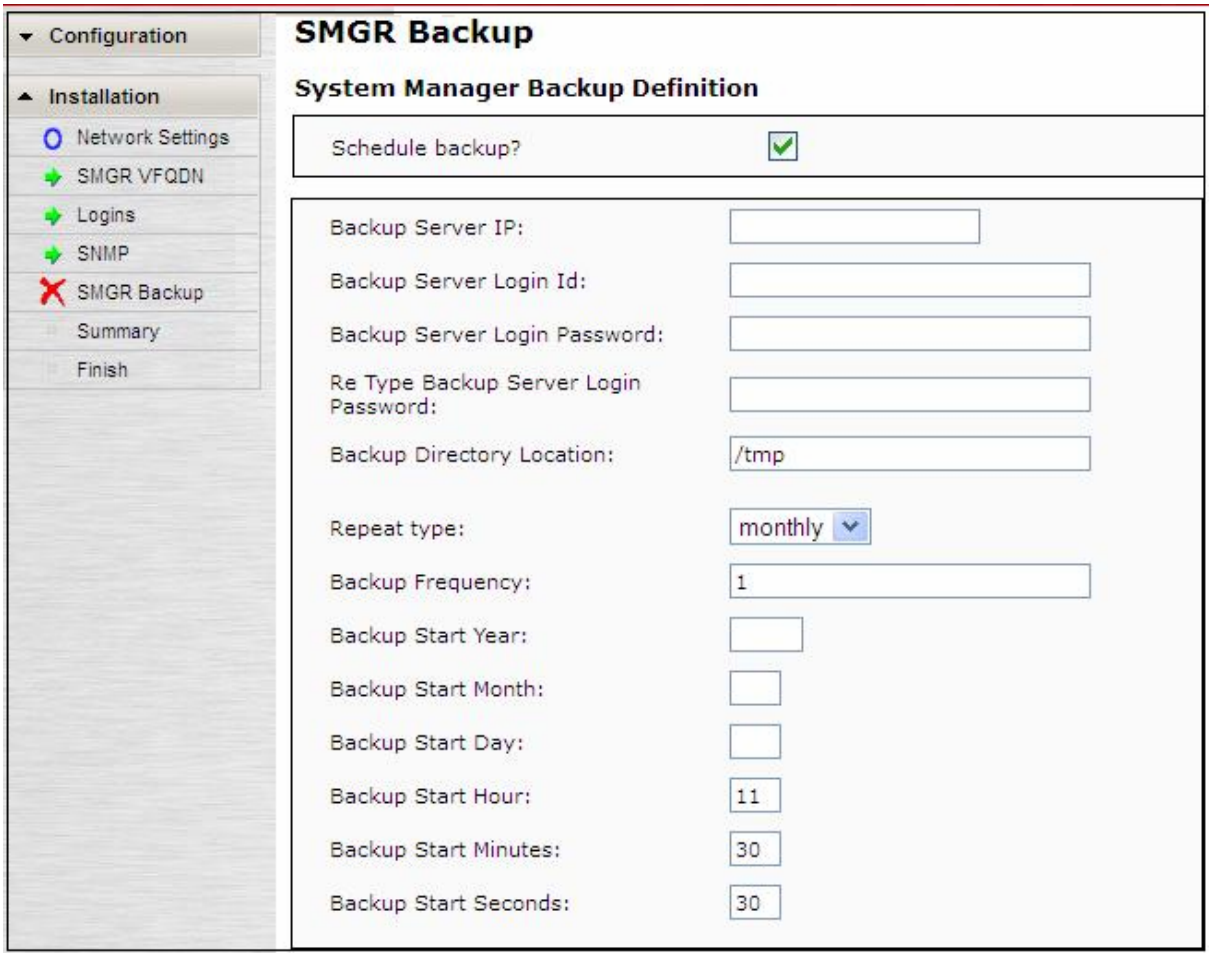
13. To navigate to the Logins page, click **Next Step**.

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

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



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



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

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

Note:

- If the system does not display the progress bar when you run the post installation script, wait for the installation to complete.

Next steps

- To gain access to the System Manager web console, perform one of the following:
  - On the web browser, type `https://<Fully qualified domain name of System Manager>`.
  - On the System Platform web console, click **Home** > **Virtual Machine List**, and click the wrench icon ( ) adjacent to the SMGR link.

    The system displays the System Manager Login page.
- (Optional) Configure the system as a secondary System Manager.

  For information about Geographic Redundancy, see *Administering Avaya Aura® System Manager*.

Upgrading System Manager to a Geographic Redundancy setup

About this task

Use the procedure to upgrade System Manager from a non-GR system to a Geographic Redundancy setup on a primary System Manager server. If you configure Geographic Redundancy on an upgraded System Manager server, the system might overwrite the data with data from the primary System Manager server.

Procedure

1. Upgrade the primary System Manager server to Release 6.3.18.

   For instructions, see the appropriate upgrade procedure in this document.
2. On the standalone System Manager server that you designate as the secondary server, install the System Manager 6.3 template.

   For installation instructions, see *Deploying Avaya Aura® System Manager on System Platform* from the Avaya Support website at http://support.avaya.com.
3. Verify that the version of the System Manager software is the same on the primary and secondary servers.
4. Install the `System_Manager_6.3.18_r5505487.bin` file on the primary System Manager server first and then on the secondary System Manager server.

Upgrading System Manager in Geographic Redundancy setup to Release 6.3.18 in Geographic Redundancy

About this task

Use the key tasks to upgrade System Manager Geographic Redundancy (GR) setup to System Manager Release 6.3.18.

Procedure

1. Disable the Geographic Redundancy replication.
2. Note the software version of System Manager on the server.
3. Create a remote System Manager backup by using the web console of the primary System Manager server.
4. Using the System Platform web console, install the `System_Manager_6.3.18_r5505487.bin` file on the primary System Manager server.
5. Install the same file on the secondary System Manager server.
6. Verify that the version of the System Manager software is the same on the primary and secondary servers.
7. Enable the Geographic Redundancy replication.

Installing patches on System Manager servers configured for Geographic Redundancy

Before you begin

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

Procedure

1. Log on to the System Manager web console of the primary System Manager.
2. Disable the Geographic Redundancy replication.

   For instructions, see Disabling the Geographic Redundancy replication. If the Geographic Redundancy replication is disabled successfully, the system displays `Disabled` in the **Disable GR Status** section.
3. 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.

4. 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 to the primary System Manager, click the settings icon () and click **About**.

      The system displays the latest patch details of System Manager.

   d. Log on to the System Platform web console, and click **Commit**.
5. To install the System Manager patch on the secondary System Manager server, perform the following:
   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 to the secondary System Manager, and 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 the System Platform web console, and click **Commit**.
6. Log on to the System Manager web console of the primary System Manager, enable the Geographic Redundancy replication.

   For instructions, see Enabling the Geographic Redundancy replication. If the Geographic Redundancy replication is enabled successfully, the system displays `Enabled` in the **Enable GR Status** section.
7. To verify the Geographic Redundancy setup, perform the following steps:
   a. Click **Administators** > **Elements**.
   b. Click the secondary System Manager server link.

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

Related links

Creating a backup of the System Manager data through System Platform on page 46
Installing patches on page 45

Upgrading the System Manager template

Before you begin

- Install the required System Platform release and the software patches that System Manager Release 6.3.18 requires.
- Get the minimum System Manager data. For example, the number of users and roles that exist in the current release of System Manager.

About this task

Use this procedure to upgrade System Manager by using an ISO file.

Important:

Do not upgrade System Manager from a specific release to the same release, for example, System Manager Release 6.3 to 6.3. This upgrade might make System Manager unusable.

Procedure

1. To log on to the System Platform web console:
   a. In the web browser, type `https://<IPAddress of the C-dom web console>`.
   b. Use the administrator credentials made available at the time of the System Platform installation.
2. In the left navigation pane, click **Virtual Machine Management** > **Templates** > **Install**.
3. Click **Upgrade**.
4. On the Search Local and Remote Template page, select an appropriate installation mode.

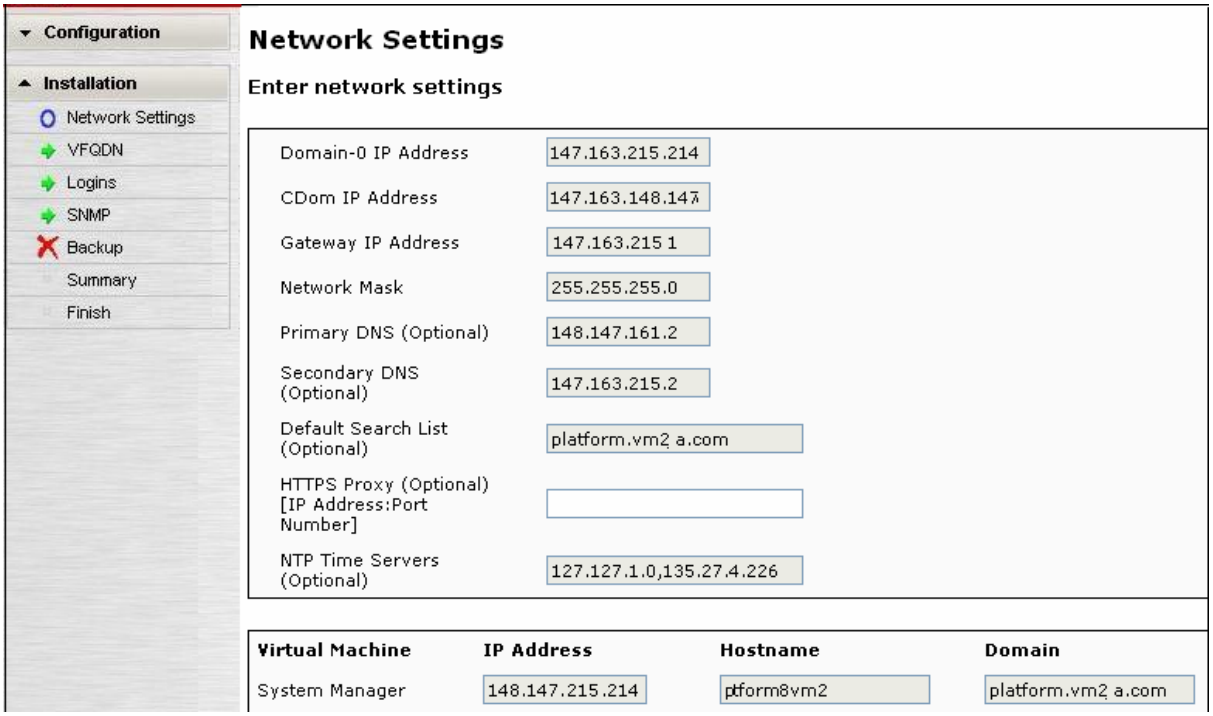
   Note:

   You can download the installation files from the Avaya Support website or extract the 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 about selecting a template, see Search Local and Remote Template field descriptions section in *Administering Avaya Aura® System Manager*.
5. To search the installation OVF file, click **Search**.
6. In the **Select Template** field, click the `SystemManager.ovf` file, and click **Select**.
7. On the Select Template page, click **Continue without EPW file** > **Upgrade**.

   The system starts the installation and displays the Network Settings page after the completion of the Pre-Install Web Application Deployment phase.
8. Click **Upgrade**.
9. **(Optional)** To cancel the upgrade process, click **Cancel Installation**. Follow the system prompts and click **OK** to cancel the upgrade process.
10. On the Network Settings page, perform the following:
    a. In **Domain**, type the domain name that was currently configured on the server.

b. In **IP Address** field, retain the address that the system automatically populates in the field.

c. In the **Hostname** field, retain the host name that the system automatically populates in the field.



11. On the VFQDN page, change the default values in the following field:

a. **Virtual Hostname**: enter a unique host name.

b. **Virtual Domain**: enter a unique domain name.

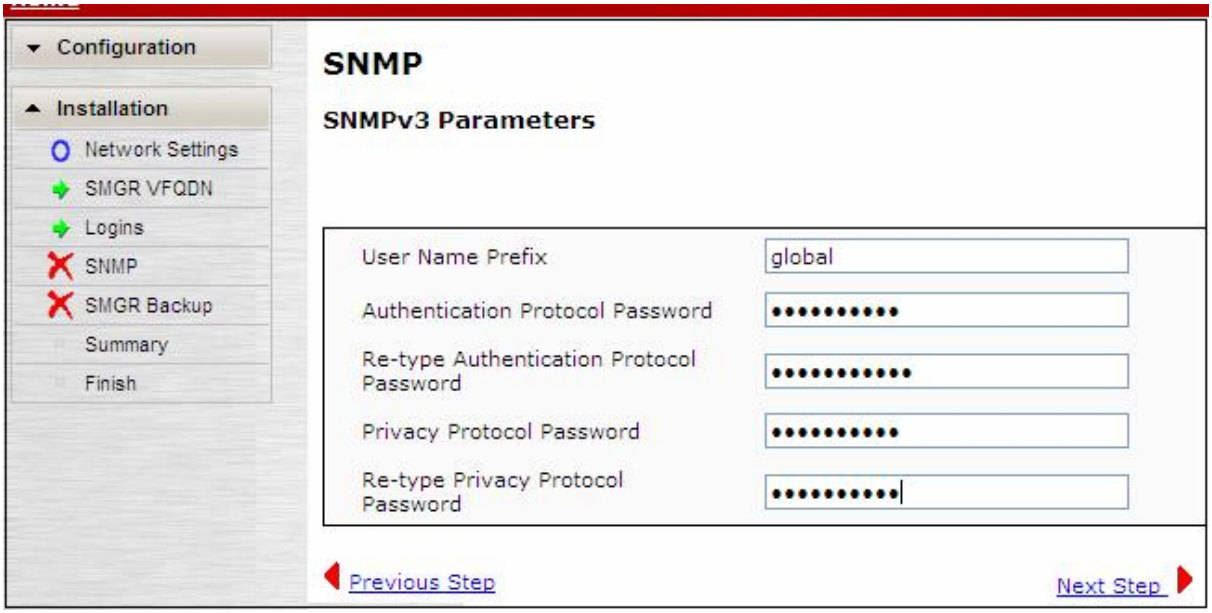
Note:

- The VFQDN value must be unique and different from the FQDN value of System Manager and the elements.
- VFQDN is a mandatory field.
- Do not add VFQDN entries in the DNS configuration.
- Do not add VFQDN in the `/etc/hosts` file on System Manager. Adding VFQDN in the `/etc/hosts` file might cause failures.
- In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN.
- After the System Manager installation, you cannot change the VFQDN unless you reinstall System Manager.

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

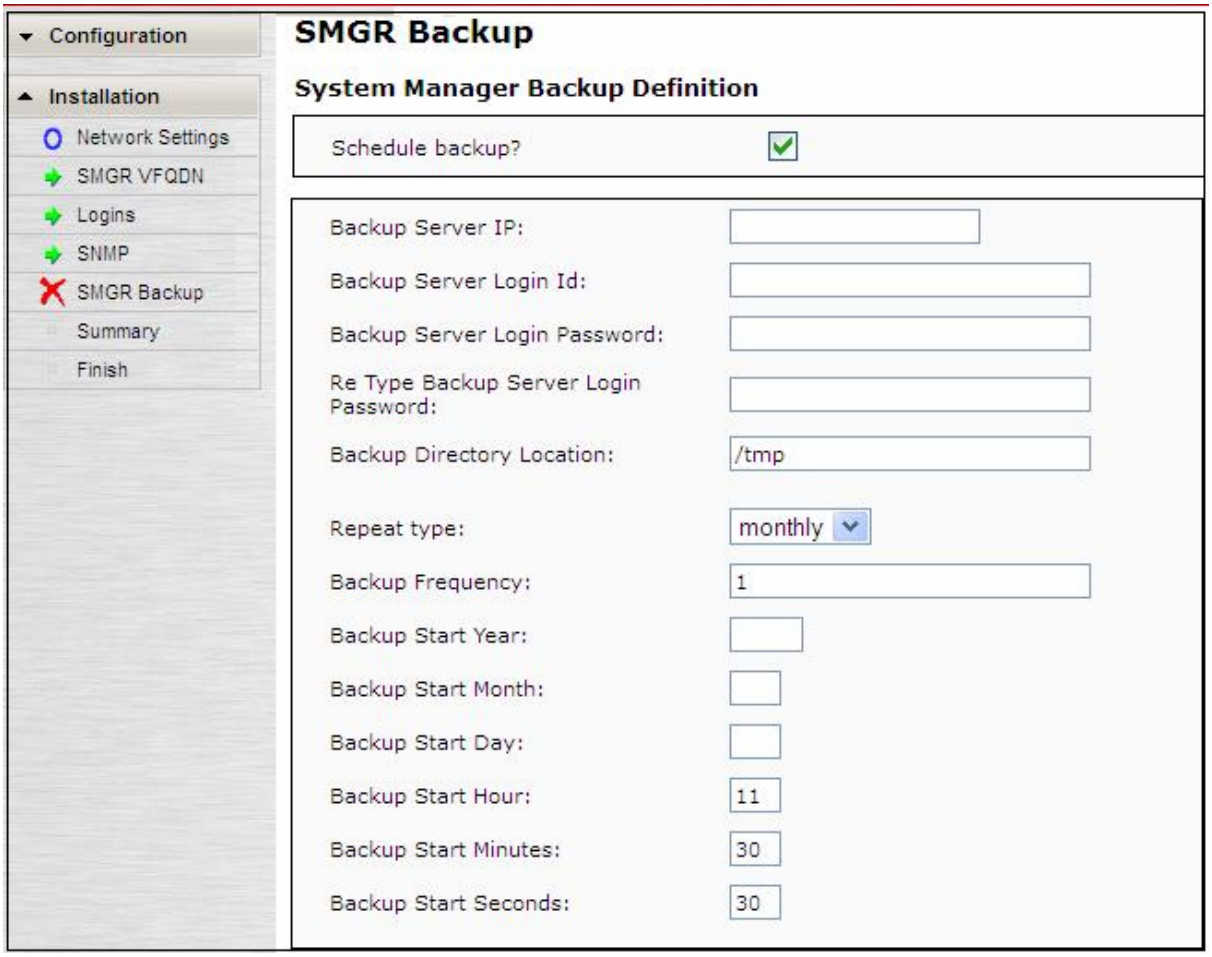
    The system displays **admin** as the default value in the **Non-root User** field.

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



14. Click **Next Step**.

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



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

    If you do not fill any of the mandatory fields in the installation screens, the system disables the **Install** button. The system completes the upgrade process.

20. To verify that the upgrade is successful, perform the following:

    a. To log on to the System Manager web console, open a new web browser and type `https://Fully qualified domain name/SMGR`.

    b. Verify that the system successfully imported the users and roles from the earlier release of System Manager to the upgraded system.

       For information, see Verifying the System Manager functionality.

Important:

Click **Commit Installation** only after you verify that the system upgraded the data successfully.

21. Click **Commit Installation**.

    If the verification procedure fails, click **Rollback Installation**.

Next steps

- Install the `System_Manager_6.3.18_r5505487.bin` file.
- Regenerate and reimport the third-party certificate.
- Verify if the system has successfully imported the data from the earlier release to the new release. For example, verify the number of users and roles that the system imported to System Manager Release 6.3.18.

Related links

Managing the third-party certificate for upgrade on page 151
Verifying the functionality of System Manager on page 259

Upgrading System Manager with a DVD

Use this procedure to upgrade System Manager using a DVD.

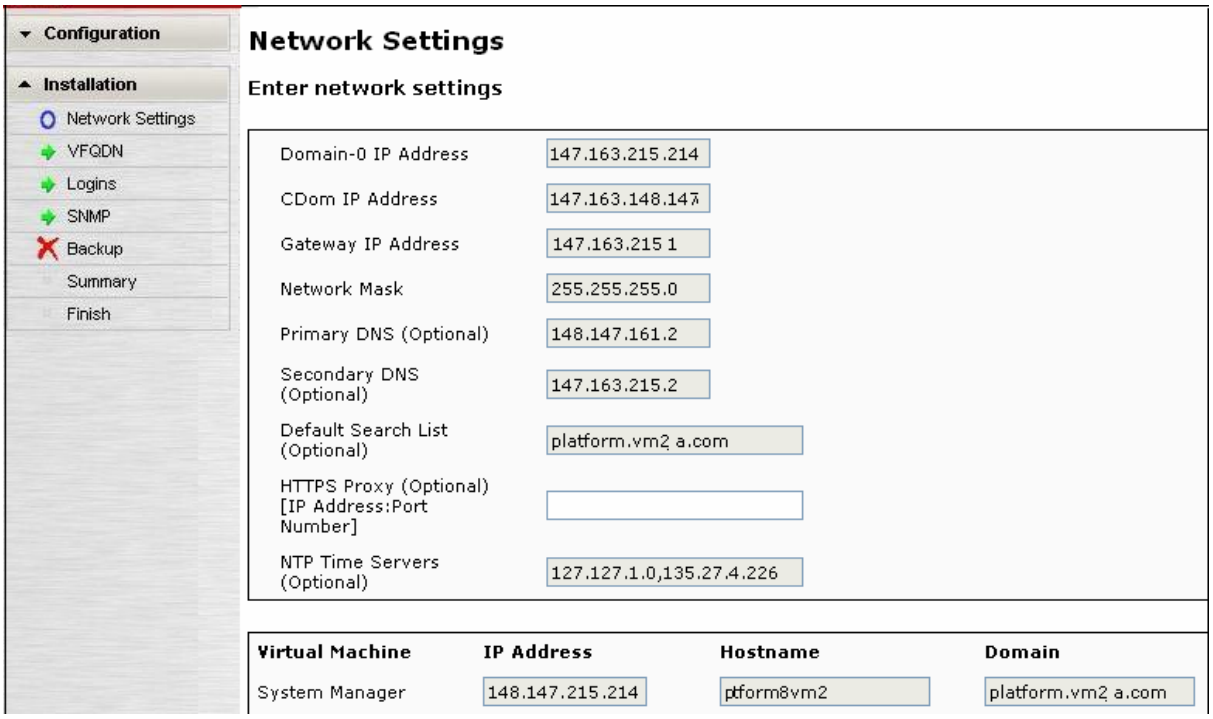
Procedure

1. Insert the DVD in the DVD drive of the server.
2. Log on to System Platform Web Console.
3. In the left navigation pane, click **Virtual Machine Management** > **Templates** > **Install**.
4. Click **Upgrade**.

   The system displays a message that prompts for a confirmation to continue with the upgrade.
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 click **Select**.
8. On the Select Template page, click **Continue without EPW file** > **Upgrade**.

   The system starts the installation and displays the Network Settings page after the completion of the Pre-Install Web Application Deployment phase.
9. Click **Upgrade**.
10. **(Optional)** To cancel the upgrade process, click **Cancel Installation**. Follow the system prompts and click **OK** to cancel the upgrade process.

11. On the Network Settings page, perform the following:
    a. In **Domain**, type the domain name that was currently configured on the server.
    b. In **IP Address** field, retain the address that the system automatically populates in the field.
    c. In the **Hostname** field, retain the host name that the system automatically populates in the field.



12. On the VFQDN page, change the default values in the following field:
    a. **Virtual Hostname**: enter a unique host name.
    b. **Virtual Domain**: enter a unique domain name.

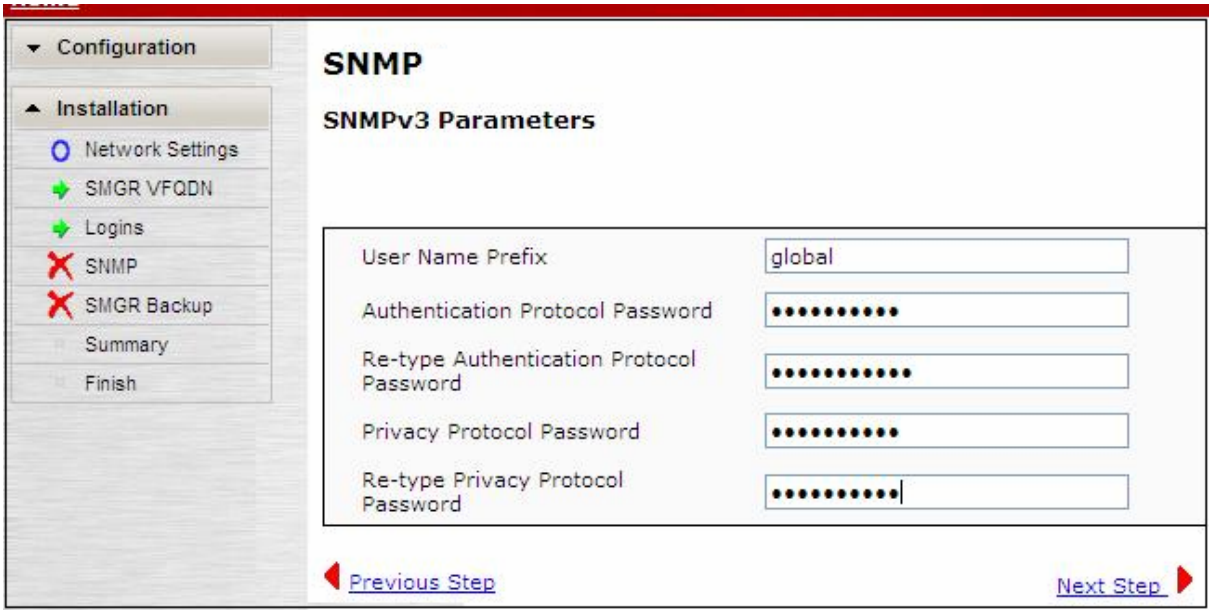
Note:

- The VFQDN value must be unique and different from the FQDN value of System Manager and the elements.
- VFQDN is a mandatory field.
- Do not add VFQDN entries in the DNS configuration.
- Do not add VFQDN in the `/etc/hosts` file on System Manager. Adding VFQDN in the `/etc/hosts` file might cause failures.
- In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN.
- After the System Manager installation, you cannot change the VFQDN unless you reinstall System Manager.

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

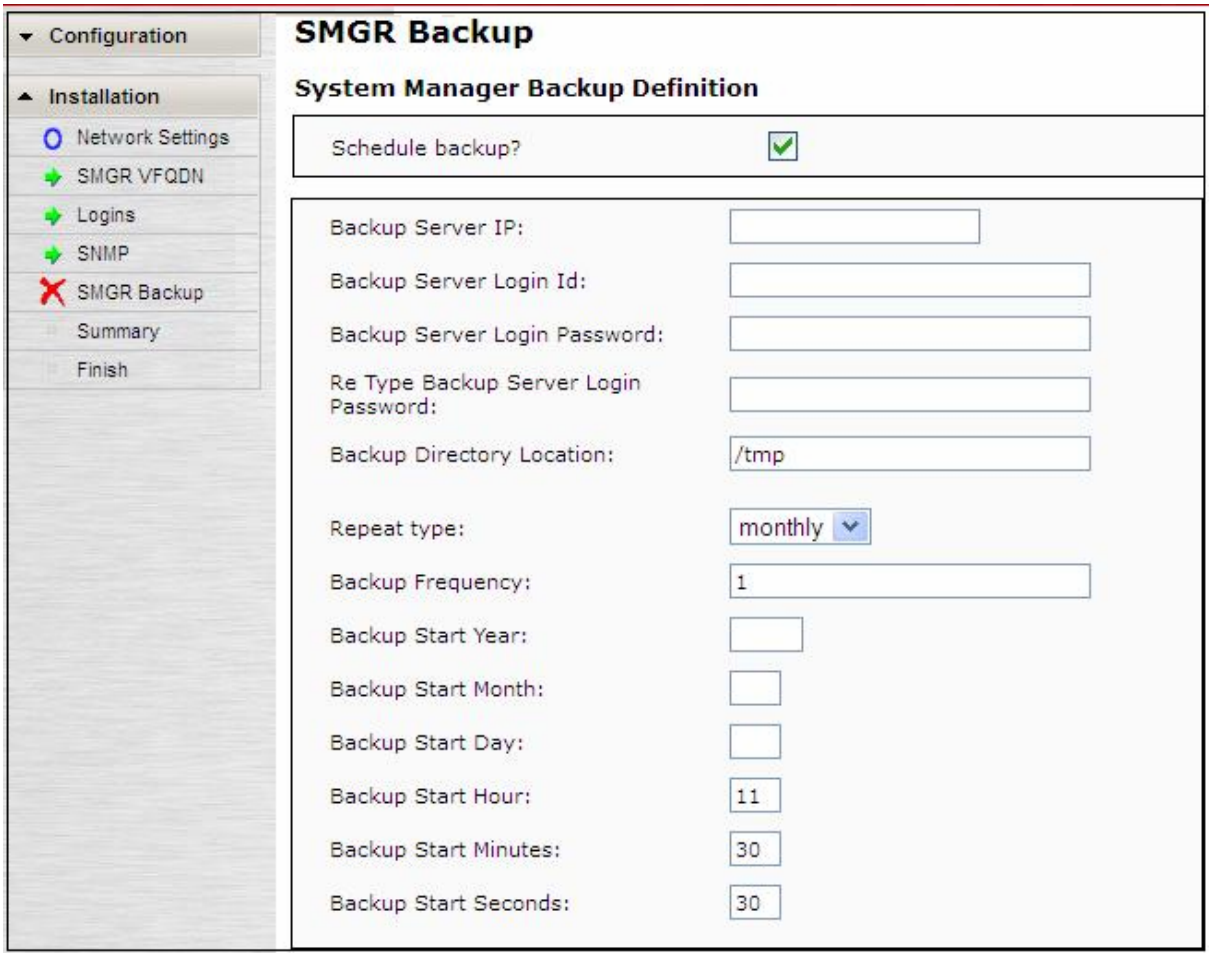
    The system displays **admin** as the default value in the **Non-root User** field.

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



15. Click **Next Step**.

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



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 screens, the system disables the **Install** button. The system completes the upgrade process.

21. To verify that the upgrade is successful, perform the following:

    a. To log on to the System Manager web console, open a new web browser and type `https://Fully qualified domain name/SMGR`.

    b. Verify that the system successfully imported the users and roles from the earlier release of System Manager to the upgraded system.

       For information, see Verifying the System Manager functionality.

Important:

Click **Commit Installation** only after you verify that the system upgraded the data successfully.

22. Click **Commit Installation**.

    If the verification procedure fails, click **Rollback Installation**.

Next steps

- Install the `System_Manager_6.3.18_r5505487.bin` file.
- Regenerate and reimport the third-party certificate.

Related links

Managing the third-party certificate for upgrade on page 151
Verifying the functionality of System Manager on page 259

Managing the third-party certificate for upgrade

Use this procedure if you are upgrading System Manager from earlier releases to Release 6.3.

About this task

The upgrade process retains the third-party identity certificate that System Manager used before the upgrade. As Subject Alternative Name in the System Manager certificate does not contain the virtual FQDN, when you upgrade Session Manager servers to Release 6.3, the replication to Session Manager servers stops.

If System Manager uses third-party identity certificate before the upgrade, you must regenerate and reimport the third-party identity certificate after you complete the System Manager upgrade.

Procedure

1. Verify the virtual FQDN that you configured in the System Manager certificate.
   a. Click **Certificate Error** next to the address bar.
   b. Click **View Certificates** > **Details** > **Subject Alternative Name**.

      The first entry in the **DNS Name** field is the virtual FQDN.
2. Generate the new identity certificate for System Manager.

   For instructions to generate the certificate, see Managing certificates in *Administering Avaya Aura® System Manager*.
3. Import the third-party identity certificate that you must add as a trusted certificate in the trust store of the element.

   For instructions to import the certificate, see Managing certificates in *Administering Avaya Aura® System Manager*.

Removing the System Manager template

Procedure

1. To log on to the C-dom Web Console of System Platform:
   a. In the Web browser, enter `https://<IPAddress>/webconsole`, where *<IPAddress>* is the IP address of C-dom.
   b. Log on to the C-dom Web Console using the administrator credentials made available at the time of the System Platform installation.
2. Perform one of the following tasks:
   - For releases earlier than System Manager Release 6.2, in the left navigation pane, click **Virtual Machine Management** > **Solution Template**.
   - For System Manager Release 6.2 and later, in the left navigation pane, click **Virtual Machine Management** > **Templates**.
3. To delete the System Manager template, perform one of the following tasks:
   - For releases earlier than System Manager Release 6.2, click **Delete Installed Template**.
   - For System Manager Release 6.2 and later, click **Delete**.
4. On the confirmation dialog box, click **OK**.

   The system deletes the System Manager template.

Chapter 5: Upgrading System Manager using the data migration utility

Data migration utility

Use the data migration utility to migrate the backup data of System Manager 6.x to System Manager Release 6.3.8. You can then upgrade to the System Manager version you want.

Use the data migration utility process to upgrade across multiple releases. For example, upgrades from Release 6.0 to Release 6.3.18.

In the data migration utility method, the system does not:

- Support the rollback operation.

  To recover data, perform the cold standby procedure for software-only upgrades and start the existing server for hardware upgrades.
- Import System Platform and the Services VM data.

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 6.3.18:

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

Prerequisites

Serial Number	Prerequisite	Notes
1	Download the following software from the Avaya Support website at http://support.avaya.com: • System Platform Release 6.3.7.0.05001 • The System Manager Release 6.3 template • The `DMUtility_6.3.8_r24.bin` file • System Manager Release 6.3.8 and Release 6.3.18 bin files	
2	Verify that the existing server is compatible with System Manager Release 6.3.18. If the existing server is incompatible, change the server as instructed in the workflow described in this chapter.	Release 6.3.x supports the following servers: • Avaya S8800 1U • Dell™ PowerEdge™ R610 2CPU MID2 • HP ProLiant DL360 G7 2CPU MID4 • Dell™ PowerEdge™ R620 • HP ProLiant DL360p G8
3	Keep the following checklists: • 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 upgrade, you require this data to verify if the system has successfully imported the users and roles from the earlier release to System Manager Release 6.3.18.	See Managing users and Managing roles in *Administering Avaya Aura® System Manager*.

Upgrade worksheet

Use the following worksheet to record the data that you will need during the upgrade.

Serial Number	Field	Value	Notes
1	**IP address of external device for remote backup**		On the remote backup page of System Manager Web Console, enter the IP address of the remote server on which you saved the backup file.
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 for the account on System Manager Web Console.
3	**System Manager command line interface credential**		Open an SSH session and enter `admin` as the user name and password.
4	**Root password of System Manager**		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 upgrading from System Manager 6.x using the data migration utility

Data migration from System Manager Release 6.0.x, 6.1.x, or 6.2.x to Release 6.3.18 involves the following tasks:

Serial Number	Task	Notes	✔
1	Check the RAID Controller battery level. 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	

Table continues…

Serial Number	Task	Notes	✔
		duration of the upgrade process increases. For additional information, see the S8800 or HP ProLiant DL360p G8 server RAID on the Avaya Support website at http://support.avaya.com/.	
2	Verify the software version of the current System Manager.	-	
3	Create a backup of System Manager and copy to the remote server.	-	
4	Record the System Platform configuration data such as SAL Gateway configuration, static routes, High Availability (HA) configuration data, and users.	Use data to reconfigure the new System Platform installation.	
5	In the High Availability (HA) setup, stop HA on the active and standby System Manager servers.	See High Availability start/stop.	

6	Record the IP address or FQDN and the system parameters.	In the command line interface, type the following commands for the details:
		`# ifconfig eth0 | grep inet`
		The system displays `inet addr:xxx.xxx.xxx.xxx Bcast:xxx.xxx.xxx.xxx Mask:xxx.xxx.xxx.xxx.`
		`#admin >hostname`	

7	If the existing server is not compatible with System Manager Release 6.3.18, change the server.	Release 6.3.18 supports the following servers: • Avaya S8800 1U • Dell™ PowerEdge™ R610 2CPU MID2 • HP ProLiant DL360 G7 2CPU MID4 • Dell™ PowerEdge™ R620 • HP ProLiant DL360p G8	
8	For hardware upgrades, install the System Platform Release 6.3.7.0.05001 software on the supported server.	For more information, see: • *Installing the HP ProLiant DL360p G8 Server* or *Installing the Dell™ PowerEdge™ R620 Server*. • Installing System Platform on page 55.	

Table continues…

Serial Number	Task	Notes	✔
		Note: If the existing system has High Availability (HA) configured on it, stop HA. You can also start the System Platform installation on the standby server. For more information, see Stopping System Platform High Availability on page 108.	
9	Install the System Manager Release 6.3 template. **Note:** System Manager hostname is case-sensitive. The restriction applies only during the upgrade of System Manager.	Installing the System Manager Release 6.3 template using ISO on page 136	
10	Copy the backup file, 6.3.8 and Release 6.3.18 bin files, and the data migration utility to the `/home/admin` location on System Manager.	-	
11	Install the System Manager Release 6.3.8 bin file. The patch installation takes about 65–70 minutes to complete on the primary and the secondary System Manager server.	Installing the System Manager Release 6.3.18 bin file on page 164	
12	On the System Manager 6.3.8 command line interface, run **`upgradeSMGR`** with `DMUtility_6.3.8_r24.bin` and the service pack or feature pack as inputs.	Upgrading to System Manager 6.3.x by using the data migration utility on page 161	
13	Verify that System Manager is functional.	Verifying the functionality of System Manager on page 163	
14	Install the `System_Manager_6.3.18_r5505487.bin` file. The patch installation takes about 65–70 minutes to complete on the primary and the secondary System Manager server.	Installing the System Manager Release 6.3.18 bin file on page 164	
15	To get the updated kernel that is running in the memory, reboot System Manager.	-	

Table continues…

Serial Number	Task	Notes	✔
16	Reconfigure System Platform with the data that you recorded in Step 4. You can also start HA. For information, see Starting System Platform High Availability on page 107.	-	
17	In the High Availability (HA) setup, start HA on the active and standby System Manager servers.	See High Availability start/stop.	
18	Create a backup of System Manager and copy to the remote server.	Creating a data backup on a remote server on page 48	

You can set up Geographic Redundancy on the system after you upgrade the system to Release 6.3.18. For information, see Geographic Redundancy in *Administering Avaya Aura® System Manager*.

Checklist for upgrade from System Manager configured with Geographic Redundancy

The data migration from System Manager in the Geographic Redundancy setup to Release 6.3.18 procedure includes the following tasks:

S No	Field	Notes	✔
1	Download the `DMUtility_6.3.8_r24.bin` file and the System Platform patch from the Avaya Support website at http://support.avaya.com.	For the latest service packs and software patches, see System Manager release notes on the Avaya Support website at http://support.avaya.com.	
2	Verify the software version of the current System Manager.		
3	Create a backup of System Manager and copy to the remote server.		
4	Keep a copy of the license files for the Avaya Aura® products so you can replicate with the new Host ID after the OVA file installation. Ensure that the license file copies are accessible.	-	
5	Disable the Geographic Redundancy replication.	See *Administering Avaya Aura® System Manager*.	
6	Install the System Manager Release 6.3.8 bin file.	Installing the System Manager Release 6.3.18 bin file on page 164	

Table continues…

S No	Field	Notes	✔
	The patch installation takes about 65–70 minutes to complete on the primary and the secondary System Manager server.		
7	Run the `DMUtility_6.3.8_r24.bin` file. The upgrade takes about 80–90 minutes. However, the duration depends on the factors such as the number of users, backup size, hardware used, and the number of resources shared during the upgrade.	Upgrading to System Manager 6.3.x by using the data migration utility on page 161	
8	Verify that System Manager is functional.	-	
9	Install the `System_Manager_6.3.18_r5505487.bin` file. In the Geographic Redundancy setup, complete the installation on the primary System Manager first and then perform on the secondary Geographic Redundancy.	Installing the System Manager Release 6.3.18 bin file on page 164 **Note:** The upgrade process on the primary System Manager takes about 65–70 minutes and about 75–80 minutes on the secondary System Manager. Wait until the upgrade process is complete, and continue with the next step.	
10	On the primary System Manager server, enable the Geographic Redundancy replication.	See *Administering Avaya Aura® System Manager*.	

For Geographic Redundancy-related procedures, see *Administering Avaya Aura® System Manager*.

Verifying the current software version

About this task

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

Procedure

1. Log on to the System Manager web console.
2. To view the build number, in the upper-right corner of the web console, click the **About** link.

   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 links

System Manager and System Platform patches on page 20
Compatibility matrix for the System Manager and System Platform software versions on page 22

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!!`

Installing System Platform

Before you begin

Log on to the System Platform web console.

Procedure

1. Download the System Platform Release 6.3.7.0.05001 software from the Avaya Support website at http://support.avaya.com.
2. On the server, install System Platform Release 6.3.7.0.05001. For instructions, see Installation methods.

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

Next steps

(Optional) If this System Platform release requires a patch, install the required System Platform patch. For the patch information, see **Required patch** column in the “Compatibility matrix for the System Manager and System Platform software versions”.

Related links

Installing patches on page 45
Compatibility matrix for the System Manager and System Platform software versions on page 22
Upgrading a System Platform server on page 121
Installation checklist for System Platform on page 55

Installing the System Manager template

Before you begin

Download the software for the System Manager 6.3 template.

Procedure

1. To log on to the System Platform web console:
   a. In the web browser, type `https://<IPAddress of the C-dom web console>`.
   b. Use the administrator credentials made available at the time of the System Platform installation.
2. Install the System Manager template. For instructions, see Installing the System Manager template.

Next steps

To gain access to the System Manager web console, perform one of the following:

- On the web browser, type `https://<Fully qualified domain name of System Manager>`.
- On the System Platform web console, click **Home** > **Virtual Machine List**, and click the wrench icon () adjacent to the SMGR link.

  The system displays the System Manager Login page.

Related links

System Manager and System Platform patches on page 20
Installing the System Manager Release 6.3 template using ISO on page 136

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

Before you begin

- Ensure that System Manager is running.
- Download `DMUtility_6.3.8_r24.bin`, `System_Manager_6.3.8_r4502376.bin`, and `System_Manager_6.3.18_r5505487.bin` files from the Avaya Support website at http://support.avaya.com.

Procedure

1. Log on to the System Manager web console.
2. Record the software version of System Manager from the **About** link.
3. Create the System Manager data backup using System Manager or the System Platform web console and copy the backup to the remote server.

4. Log in to the System Manager command line interface of the existing system.
5. Shut down System Manager.
6. Install the System Manager Release 6.3 template.

   Important:

   Use the same network parameters and system parameters that you recorded on the existing system.

7. Copy `DMUtility_6.3.8_r24.bin`, System Manager backup file, `System_Manager_6.3.8_r4502376.bin`, and `System_Manager_6.3.18_r5505487.bin` files to the `/home/admin` location on System Manager.
8. To log in to the System Manager virtual machine as the root user, type `su - root`.
9. Do one of the following:
   - From System Platform, install the `System_Manager_6.3.8_r4502376.bin` file.

     For more information, see Installing the System Manager 6.3.8 release notes.
   - From the command line interface, copy the `System_Manager_6.3.8_r4502376.bin` file to System Manager by using software that supports SCP, and type `sh <System Manager bin file name>.bin`.
10. At the prompt, do the following:
    a. To remove any older data migration utility-related files, type `rm -fr /opt/Avaya/data_migration`.
    b. Type `sh /home/admin/DMUtility_6.3.8_r4.bin -m -v`.
    c. Type the absolute path to the backup file:

       ```
       /home/admin/<backupfile name.*>
       ```

       The system displays the following message:

       ```
       Verified that the file /home/admin/<backupfile name>.zip exists.
       You are about to run the System Manager Data Migration utility.
       The System Manager will be inaccessible for approx. 90 mins,
       depending on the resources available on the system.
       ```

11. Log on to System Manager and verify that the upgrade is successful.
12. At the prompt, run the following command to install the Release 6.3.18 bin file:

    ```
    SMGRPatchdeploy <absolute path to the System_Manager_6.3.18_r5505487.bin file>
    ```

    The patch installation takes about 60–65 minutes to complete.

Related links

Installing the System Manager Release 6.3.18 bin file on page 164

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

   See Managing users and Managing roles 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 more information on completing each verification task, see *Administering Avaya Aura® System Manager*.

Installing the System Manager Release 6.3.18 bin file

Before you begin

- Log on to the System Platform web console.
- Download the `System_Manager_6.3.18_r5505487.bin` file from the Avaya support website at http://support.avaya.com.

  For more information, see Downloading patches.

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, select the `System_Manager_6.3.18_r5505487.bin` file.
4. On the Patch Detail page, click **Install**.
5. To verify that the patch installation is successful, on the System Manager web console, at the upper-right corner, click the settings icon () and click **About**.
6. Click **Commit**.

Next steps

To get the updated kernel that is running in the memory, restart System Manager

Related links

Installing patches on page 45
Downloading patches on page 43

Creating a data backup on a remote server

Procedure

1. On the 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:
     a. In the **File transfer protocol** field, click `SCP` or `SFTP`.
     b. Enter 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, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can 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 links

System Manager data backup options on page 49

SSO login to remote machine fails

For System Manager deployments that involve remote machines such as CS 1000 Servers and solutions based on the System Manager Single Sign On (SSO) client, the Web-based Single Sign On between System Manager and the remote machine fails.

During the data migration or IP-FQDN change, the system does not import the LDAP attribute that contains the SSO cookie domain value back to the directory. Therefore, the System Manager SSO login to the remote machine fails. Enable SSO after the data migration or the IP-FQDN change.

Related links

Reimporting the SSO cookie domain value on page 165

Reimporting the SSO cookie domain value

Procedure

1. On the System Manager web console, click **Users** > **Administrators**.
2. In the left navigation pane, click **Security** > **Policies**.
3. In the section **Single Sign-on Cookie Domain** section, click **Edit**.
4. In the **Single Sign-on Cookie Domain** field, select an appropriate domain based on the FQDN of the servers that you deployed.
5. Click **Save**.

Data migration from System Manager 5.2

Overview

Use this section to upgrade System Manager Release 5.2, 5.2 SP1, or 5.2 SP2 to Release 6.3.18 running on System Platform.

During the upgrade from System Manager Release 5.2.x to Release 6.3.18, the system only retains the routing data. You must manually add the remaining System Manager data to the Release 6.3.18 system.

NRP import and export utility

Use the NRP import and export utility to import and export only the routing data from System Manager 5.2.x to System Manager Release 6.3.18. You cannot migrate the data related to other System Manager options.

Checklist for upgrades from System Manager Release 5.2.x

The upgrades from System Manager Release 5.2, 5.2 SP1, or 5.2 SP2 to Release 6.3.18 procedure consists the following high-level tasks. Perform the tasks sequentially.

#	Task	Notes	✔
1		-	
2		Creating a data backup on a remote server on page 168	
3	Export the routing data from System Manager Release 5.2.x.	-	
4		Use data to reconfigure the new System Platform installation.	

5	Record the IP address or FQDN and the system parameters.	In the command line interface, type the following commands for the details:
		`# ifconfig eth0 | grep inet`
		The system displays `inet addr:xxx.xxx.xxx.xxx Bcast:xxx.xxx.xxx.xxx Mask:xxx.xxx.xxx.xxx.`
		`#admin >hostname`	

Table continues…

#	Task	Notes	✔
6	If the existing server is not compatible with System Manager Release 6.3.18, change the server.	Release 6.2 and later supports the following servers: • Avaya S8800 1U • Dell™ PowerEdge™ R610 2CPU MID2 • HP ProLiant DL360 G7 2CPU MID4 • Dell™ PowerEdge™ R620 • HP ProLiant DL360p G8	
7	For hardware upgrades, install the System Platform Release 6.3.7.0.05001 software on the supported server.	• *Installing the HP ProLiant DL360p G8 Server* or *Installing the Dell™ PowerEdge™ R620 Server*. • Installing System Platform on page 55. **Note:** If the existing system has High Availability (HA) configured on it, stop HA. You can also start the System Platform installation on the standby server. For more information, see Stopping System Platform High Availability on page 108.	
8	Install the System Manager Release 6.3 template.	Installing the System Manager template using ISO on page 136.	
9	Install the `System_Manager_6.3.18_r5505487.bin` file. The patch installation takes about 65–70 minutes to complete on the primary and the secondary System Manager server.	Installing the System Manager Release 6.3.18 bin file on page 164	
10	Copy the backup file on System Manager Release 6.3.18.	-	
11	Import the data to System Manager Release 6.3.18.	Importing the data to System Manager Release 6.3.18 on page 171.	
12		Verifying the functionality of System Manager on page 163	
13	Reconfigure System Platform with the data that you recorded in Step 4. You can also start HA. For information, see Starting System Platform High Availability on page 107.	-	
14		Creating a data backup on a remote server on page 48	

Verifying the current software version on System Manager 5.2.x or earlier

Procedure

1. Log in to System Manager from the command line interface (CLI).
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 links

System Manager and System Platform patches on page 20
Compatibility matrix for the System Manager and System Platform software versions on page 22

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 routing data from System Manager 5.2.x

Before you begin

- Create a backup of System Manager 5.2.x and copy to the remote server.
- Record the NRP records on System Manager 5.2.x. 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 6.3.18.

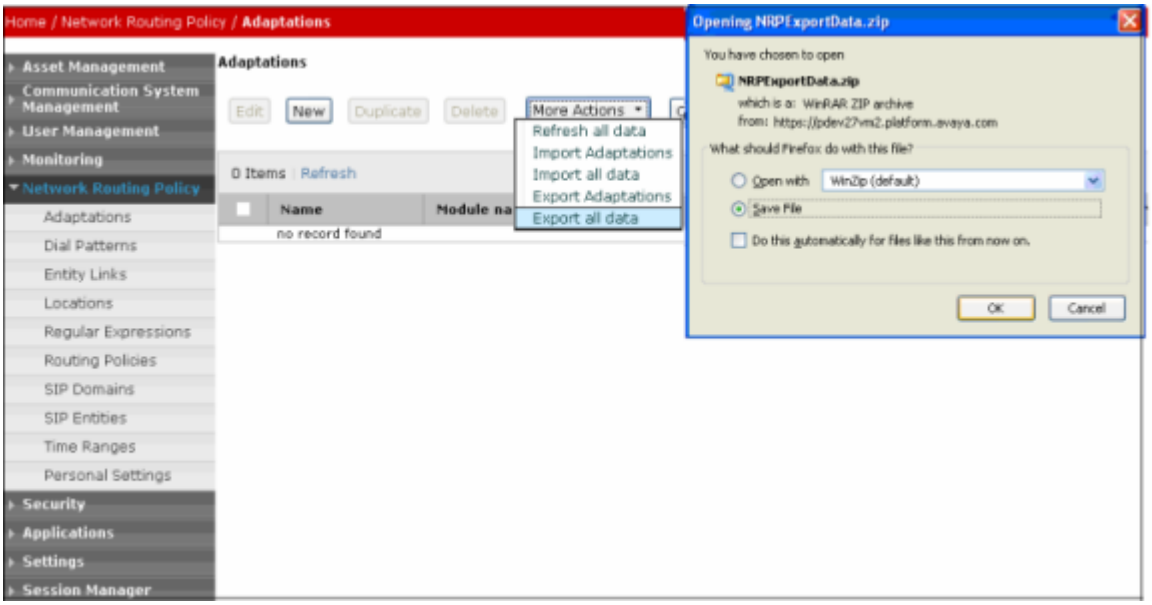
- Record the data related to users, custom roles, and configuration. After importing the NRP data, you must manually add the data to System Manager Release 6.3.18.
- Record the network parameters on System Manager 5.2.x.

About this task

Use this procedure to export the System Manager routing data from Release 5.2, 5.2 SP1, or 5.2 SP2 to System Manager Release 6.3.18.

Procedure

1. On the Web browser, type `https://<IPAddress of System Manager>/SMGR` to log on to System Manager Web Console.
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**.



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 the System Platform web console.

Procedure

1. Download the System Platform Release 6.3.7.0.05001 software from the Avaya Support website at http://support.avaya.com.
2. On the server, install System Platform Release 6.3.7.0.05001. For instructions, see Installation methods.

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

Next steps

(Optional) If this System Platform release requires a patch, install the required System Platform patch. For the patch information, see **Required patch** column in the “Compatibility matrix for the System Manager and System Platform software versions”.

Related links

Installing patches on page 45
Compatibility matrix for the System Manager and System Platform software versions on page 22
Upgrading a System Platform server on page 121
Installation checklist for System Platform on page 55

Installing the System Manager template

Before you begin

Download the software for the System Manager 6.3 template.

Procedure

1. To log on to the System Platform web console:
   a. In the web browser, type `https://<IPAddress of the C-dom web console>`.
   b. Use the administrator credentials made available at the time of the System Platform installation.
2. Install the System Manager template. For instructions, see Installing the System Manager template.

Next steps

To gain access to the System Manager web console, perform one of the following:

- On the web browser, type `https://<Fully qualified domain name of System Manager>`.
- On the System Platform web console, click **Home** > **Virtual Machine List**, and click the wrench icon ( ) adjacent to the SMGR link.

  The system displays the System Manager Login page.

Related links

System Manager and System Platform patches on page 20

Installing the System Manager Release 6.3 template using ISO on page 136

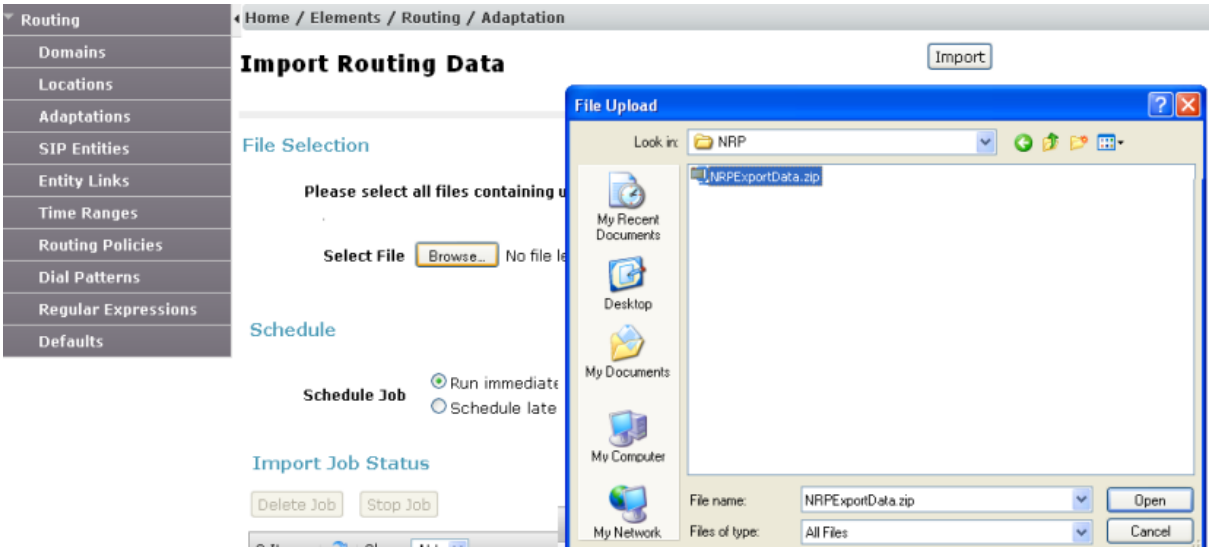
Importing the data to System Manager Release 6.3.18

Perform this procedure on System Manager 5.2.x to import the System Manager data from Release 5.2, 5.2 SP1, or 5.2 SP2 to System Manager Release 6.3.18.

Procedure

1. On the Web browser, type `https://<fully qualified domain name 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 **Elements** > **Routing** > **Adaptations**.
4. On the Adaptations page, click **More Actions** > **Import**.

   The system displays the Import Routing Data page.
5. In the File Selection section, click Browse to open 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 6.3.18.
8. Create users, custom roles, and configuration information that you recorded from the System Manager web console of Release 5.2.x.

Installing the System Manager Release 6.3.18 bin file

Before you begin

- Log on to the System Platform web console.
- Download the `System_Manager_6.3.18_r5505487.bin` file from the Avaya support website at http://support.avaya.com.

  For more information, see Downloading patches.

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, select the `System_Manager_6.3.18_r5505487.bin` file.
4. On the Patch Detail page, click **Install**.
5. To verify that the patch installation is successful, on the System Manager web console, at the upper-right corner, click the settings icon () and click **About**.
6. Click **Commit**.

Next steps

To get the updated kernel that is running in the memory, restart System Manager

Related links

Installing patches on page 45
Downloading patches on page 43

Creating a data backup on a remote server

Procedure

1. On the 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:
     a. In the **File transfer protocol** field, click `SCP` or `SFTP`.
     b. Enter 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, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can 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 links

System Manager data backup options on page 49

Chapter 6: Upgrading from System Manager 6.3, 6.3 SP1, 6.3.2, or later on a new server

Introduction

This section describes the procedure to upgrade System Manager from Release 6.3, 6.3 SP1, 6.3.2, and later to Release 6.3.18.

In this upgrade procedure, replace the server with an HP DL360 G8 or a Dell R620 Server. On the new server, install System Platform Release 6.3.7.0.05001, the System Manager Release 6.3 template, and the `System_Manager_6.3.18_r5505487.bin` file.

Checklist for upgrade from System Manager 6.3.x

Use the checklist for upgrading System Manager from Release 6.3 or 6.3 SP1 to Release 6.3.18 on System Platform:

#	Field	Notes	✔
1	Download System Manager 6.3.8, Release 6.3.18, the file and the System Platform patch from the Avaya Support website at http://support.avaya.com.	For the latest service packs and software patches, see System Manager release notes on the Avaya Support website at http://support.avaya.com.	
2	Verify the software version of the current System Manager.	-	
3	Disable the Geographic Redundancy replication only when Geographic Redundancy is already enabled on the system.	Perform only in the Geographic Redundancy setup.	
4	Create the backup of System Manager and copy the backup to a remote server.	Creating a backup of the System Manager data through System Platform on page 46	

Table continues…

#	Field	Notes	✔
5	For System Manager Release 6.3 and 6.3 SP1, upgrade System Platform to Release 6.3.7.0.05001.	See Upgrading a System Platform server.	
6	Install the `System_Manager_6.3.18_r5505487.bin` file. In the Geographic Redundancy setup, complete the installation on the primary System Manager first and then perform on the secondary Geographic Redundancy.	Installing the System Manager Release 6.3.18 bin file on page 164 **Note:** The upgrade process on the primary System Manager takes about 60–65 minutes and about 70–75 minutes on the secondary System Manager. Wait until the upgrade process is complete, and continue with the next step.	
7	Enable the Geographic Redundancy replication if you disabled on the system.	Perform only in the Geographic Redundancy setup.	
8	Verify that the version of System Manager in the **About** link is Release 6.3.18.	-	

For Geographic Redundancy-related procedures, see *Administering Avaya Aura® System Manager*.

Verifying the current software version

About this task

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

Procedure

1. Log on to the System Manager web console.
2. To view the build number, in the upper-right corner of the web console, click the **About** link.

   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 links

System Manager and System Platform patches on page 20
Compatibility matrix for the System Manager and System Platform software versions on page 22

Creating a backup of the System Manager data

Procedure

1. Log on to the System Platform web console.
2. From the System Platform web console, create a backup of the System Manager data. For instructions, see Creating a backup of the System Manager data through System Platform.

Related links

Creating a backup of the System Manager data through System Platform on page 46

Shutting down the System Platform Server

About this task

When you reboot or shut down the System Platform server, the system reboots or shuts down all the virtual machines running on System Platform. This can result in a service disruption.

Note:

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

Procedure

1. Click **Server Management** > **Server Reboot/Shutdown**.
2. On the Server Reboot/Shutdown page, click **Shutdown Server**.

Upgrade tasks on a new server

Installing System Platform

Before you begin

Log on to the System Platform web console.

Procedure

1. Download the System Platform Release 6.3.7.0.05001 software from the Avaya Support website at http://support.avaya.com.
2. On the server, install System Platform Release 6.3.7.0.05001. For instructions, see Installation methods.

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

Next steps

(Optional) If this System Platform release requires a patch, install the required System Platform patch. For the patch information, see **Required patch** column in the “Compatibility matrix for the System Manager and System Platform software versions”.

Related links

Installing patches on page 45
Compatibility matrix for the System Manager and System Platform software versions on page 22
Upgrading a System Platform server on page 121
Installation checklist for System Platform on page 55

Restoring the System Manager backup data

Before you begin

Log on to System Platform Web Console.

About this task

You can restore the backup data from System Manager that is configured for Geographic Redundancy on a standalone System Manager. However, you cannot restore the backup data from a standalone System Manager on System Manager that is configured for Geographic Redundancy.

You cannot restore the backup data on the primary System Manager server when the Geographic Redundancy replication is enabled on System Manager.

Note:

The restore operation does not restore the High Availability Failover configuration from the backup file. The restore feature does not reenable a failed High Availability Failover node back to High Availability Failover configuration. Follow the instructions given in this document on how to reenable a failed High Availability Failover node back to High Availability Failover configuration. Restore the backup configuration before configuring and starting High Availability Failover.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Restore**.
3. On the **Restore** tab, in the **Restore From** field, click `SFTP`.
4. Enter the details of the remote server on which the archive file is located:
   - **SFTP Hostname/IP**
   - **SFTP Directory**
   - **SFTP Username**
   - **SFTP Password**
5. Click **Search**.

   The system searches for archive files in the specified directory of the remote server.

6. To restore from the selected archive, select an archive file from the list, and then click **Restore**.

   The system displays the restore progress window in the Restore tab and displays restore event messages with timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - A system error condition abruptly halts the operation. In this case, contact Avaya Support at http://support.avaya.com.

   When the restore progress window displays a message indicating successful completion of the operation, the system restarts. You must log on again to the System Platform web console.

Result

After the restore is complete on System Manager that is configured for Geographic Redundancy, the system automatically restarts with the Geographic Redundancy replication status as disabled.

Installing the System Manager template

Before you begin

Download the software for the System Manager 6.3 template.

Procedure

1. To log on to the System Platform web console:
   a. In the web browser, type `https://<IPAddress of the C-dom web console>`.
   b. Use the administrator credentials made available at the time of the System Platform installation.
2. Install the System Manager template. For instructions, see Installing the System Manager template.

Next steps

To gain access to the System Manager web console, perform one of the following:

- On the web browser, type `https://<Fully qualified domain name of System Manager>`.
- On the System Platform web console, click **Home** > **Virtual Machine List**, and click the wrench icon ( ) adjacent to the SMGR link.

  The system displays the System Manager Login page.

Related links

System Manager and System Platform patches on page 20
Installing the System Manager Release 6.3 template using ISO on page 136

Installing the System Manager Release 6.3.18 bin file

Before you begin

- Log on to the System Platform web console.
- Download the `System_Manager_6.3.18_r5505487.bin` file from the Avaya support website at http://support.avaya.com.

  For more information, see Downloading patches.

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, select the `System_Manager_6.3.18_r5505487.bin` file.
4. On the Patch Detail page, click **Install**.
5. To verify that the patch installation is successful, on the System Manager web console, at the upper-right corner, click the settings icon ( ) and click **About**.
6. Click **Commit**.

Next steps

To get the updated kernel that is running in the memory, restart System Manager

Related links

Installing patches on page 45
Downloading patches on page 43

Chapter 7: Upgrading from System Manager 6.3, 6.3 SP1, 6.3.2, or later on the same server

Introduction

This section describes the procedure to upgrade System Manager from Release 6.3, 6.3 SP1, 6.3.2, or later running System Platform to Release 6.3.18.

In this upgrade procedure, you must reuse the existing server and perform the following:

- Upgrade System Platform to Release 6.3.7.0.05001.
- Install the `System_Manager_6.3.18_r5505487.bin` file.

Verifying the current software version

About this task

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

Procedure

1. Log on to the System Manager web console.
2. To view the build number, in the upper-right corner of the web console, click the **About** link.

   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 links

System Manager and System Platform patches on page 20
Compatibility matrix for the System Manager and System Platform software versions on page 22

Creating a backup of the System Manager data

Procedure

1. Log on to the System Platform web console.
2. From the System Platform web console, create a backup of the System Manager data. For instructions, see Creating a backup of the System Manager data through System Platform.

Related links

Creating a backup of the System Manager data through System Platform on page 46

Upgrading System Platform

About this task

Do not perform this procedure on System Manager Release 6.3.2 or later. You can directly install the `System_Manager_6.3.18_r5505487.bin` file on System Manager Release 6.3.2 or later to upgrade to Release 6.3.18.

Procedure

1. Download the System Platform Release 6.3.7.0.05001 software from the Avaya Support website at http://support.avaya.com.
2. Perform one of the following steps:
   - For System Manager Release 6.3 SP1, upgrade System Platform from Release 6.2.2.08001.0 to Release 6.3.7.0.05001. For instructions, see Upgrading a System Platform server.
   - For System Manager Release 6.3, upgrade System Platform from Release 6.2.2.06002.0 to Release 6.3.7.0.05001. For instructions, see Upgrading a System Platform server.

Related links

Upgrading a System Platform server on page 121

Installing the System Manager Release 6.3.18 bin file

Before you begin

- Log on to the System Platform web console.
- Download the `System_Manager_6.3.18_r5505487.bin` file from the Avaya support website at http://support.avaya.com.

  For more information, see Downloading patches.

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, select the `System_Manager_6.3.18_r5505487.bin` file.
4. On the Patch Detail page, click **Install**.
5. To verify that the patch installation is successful, on the System Manager web console, at the upper-right corner, click the settings icon () and click **About**.
6. Click **Commit**.

Next steps

To get the updated kernel that is running in the memory, restart System Manager

Related links

Installing patches on page 45
Downloading patches on page 43

Chapter 8: Upgrading from System Manager 6.2, 6.2 SP1, SP2, SP3, or SP4 on the same server

Introduction

This section describes the procedure to upgrade System Manager from Release 6.2, 6.2 SP1, 6.2 SP2, 6.2 SP3, or 6.2 SP4 running System Platform to Release 6.3.18.

In this upgrade procedure, reuse the existing server, upgrade System Platform to Release 6.3.7.0.05001, upgrade the System Manager to Release 6.3, and install the `System_Manager_6.3.18_r5505487.bin` file.

Verifying the current software version

About this task

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

Procedure

1. Log on to the System Manager web console.
2. To view the build number, in the upper-right corner of the web console, click the **About** link.

   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 links

System Manager and System Platform patches on page 20
Compatibility matrix for the System Manager and System Platform software versions on page 22

Creating a backup of the System Manager data

Procedure

1. Log on to the System Platform web console.
2. From the System Platform web console, create a backup of the System Manager data. For instructions, see Creating a backup of the System Manager data through System Platform.

Related links

Creating a backup of the System Manager data through System Platform on page 46

Upgrading System Platform

Procedure

1. Download the System Platform Release 6.3.7.0.05001 software from the Avaya Support website at http://support.avaya.com.
2. Perform one of the following steps:
   - For System Manager 6.2, upgrade System Platform from Release 6.2.0.0.27 to 6.3.7.0.05001.

     For instructions, see Upgrading a System Platform server.
   - For System Manager 6.2 SP1, upgrade System Platform from Release 6.2.0.2.27 to 6.3.7.0.05001.
   - For System Manager 6.2 SP2, upgrade System Platform from Release 6.2.1.0.9 to 6.3.7.0.05001.
   - For System Manager 6.2 SP3 or SP4, upgrade System Platform from Release 6.2.1.3.9 to 6.3.7.0.05001.

Upgrading System Manager

Before you begin

Get the System Manager Release 6.3 software from the Avaya Support site at http://support.avaya.com.

Procedure

Upgrade the System Manager template to Release 6.3. For more information, see Upgrading the System Manager template.

Next steps

For any postinstall patches that you must apply, see System Manager 6.3 release notes on the Avaya Support site at http://support.avaya.com.

Related links

Upgrading the System Manager template on page 143

Installing the System Manager Release 6.3.18 bin file

Before you begin

- Log on to the System Platform web console.
- Download the `System_Manager_6.3.18_r5505487.bin` file from the Avaya support website at http://support.avaya.com.

  For more information, see Downloading patches.

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, select the `System_Manager_6.3.18_r5505487.bin` file.
4. On the Patch Detail page, click **Install**.
5. To verify that the patch installation is successful, on the System Manager web console, at the upper-right corner, click the settings icon ( ) and click **About**.
6. Click **Commit**.

Next steps

To get the updated kernel that is running in the memory, restart System Manager

Related links

Installing patches on page 45
Downloading patches on page 43

Chapter 9: Upgrading from System Manager 6.2, 6.2 SP1, SP2, SP3, or SP4 on a new server

Introduction

This section describes the procedure to upgrade System Manager from Release 6.2, 6.2 SP1, 6.2 SP2, 6.2 SP3, or 6.2 SP4 to Release 6.3.18.

In this upgrade procedure, replace the server with an HP DL360 G8 or a Dell R620 Server. On the new server, install System Platform Release 6.3.7.0.05001, the System Manager Release 6.3 template, and the `System_Manager_6.3.18_r5505487.bin` file.

Verifying the current software version

About this task

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

Procedure

1. Log on to the System Manager web console.
2. To view the build number, in the upper-right corner of the web console, click the **About** link.

   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 links

System Manager and System Platform patches on page 20
Compatibility matrix for the System Manager and System Platform software versions on page 22

Creating a backup of the System Manager data

Procedure

1. Log on to the System Platform web console.
2. From the System Platform web console, create a backup of the System Manager data. For instructions, see Creating a backup of the System Manager data through System Platform.

Related links

Creating a backup of the System Manager data through System Platform on page 46

Shutting down the System Platform Server

About this task

When you reboot or shut down the System Platform server, the system reboots or shuts down all the virtual machines running on System Platform. This can result in a service disruption.

Note:

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

Procedure

1. Click **Server Management** > **Server Reboot/Shutdown**.
2. On the Server Reboot/Shutdown page, click **Shutdown Server**.

Upgrade tasks on a new server

Installing System Platform

Before you begin

Log on to the System Platform web console.

Procedure

1. Download the System Platform release that is compatible with the current System Manager release from the Avaya Support website at http://support.avaya.com.
2. On the server, install the System Platform software.

   For instructions, see Installation methods. The network configuration for System Platform must be the same as the network configuration of System Manager.

Next steps

(Optional) If this System Platform release requires a patch, install the patch. For the patch information, see System Manager release notes for the specific release on the Avaya Support website at http://support.avaya.com.

Installing System Manager Release 6.2, 6.2 SP1, 6.2 SP2, 6.2 SP3, or 6.2 SP4

Before you begin

- Log on to System Platform Web Console.
- Obtain the software for System Manager Release 6.2 and 6.2 SP1, 6.2 SP2, 6.2 SP3, or 6.2 SP4 patches as appropriate from the PLDS website at https://plds.avaya.com depending on the release on the existing System Manager.

Procedure

On the new server, perform one of the following:

- Install the System Manager Release 6.2 template.
- Install the System Manager Release 6.2 template and 6.2 SP1, 6.2 SP2, 6.2 SP3, or 6.2 SP4 patch.

For instructions, see *Installing and upgrading Avaya Aura® System Manager*, for the appropriate release. To download the documentation, see Downloading the documentation from the Avaya Support website.

Related links

Downloading the documentation from the Avaya Support site on page 270

Restoring the System Manager backup data

Before you begin

Log on to System Platform Web Console.

About this task

You can restore the backup data from System Manager that is configured for Geographic Redundancy on a standalone System Manager. However, you cannot restore the backup data from a standalone System Manager on System Manager that is configured for Geographic Redundancy.

You cannot restore the backup data on the primary System Manager server when the Geographic Redundancy replication is enabled on System Manager.

Note:

The restore operation does not restore the High Availability Failover configuration from the backup file. The restore feature does not reenable a failed High Availability Failover node back to High Availability Failover configuration. Follow the instructions given in this document on how

to reenable a failed High Availability Failover node back to High Availability Failover configuration. Restore the backup configuration before configuring and starting High Availability Failover.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Restore**.
3. On the **Restore** tab, in the **Restore From** field, click `SFTP`.
4. Enter the details of the remote server on which the archive file is located:
   - **SFTP Hostname/IP**
   - **SFTP Directory**
   - **SFTP Username**
   - **SFTP Password**
5. Click **Search**.

   The system searches for archive files in the specified directory of the remote server.
6. To restore from the selected archive, select an archive file from the list, and then click **Restore**.

   The system displays the restore progress window in the Restore tab and displays restore event messages with timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - A system error condition abruptly halts the operation. In this case, contact Avaya Support at http://support.avaya.com.

   When the restore progress window displays a message indicating successful completion of the operation, the system restarts. You must log on again to the System Platform web console.

Result

After the restore is complete on System Manager that is configured for Geographic Redundancy, the system automatically restarts with the Geographic Redundancy replication status as disabled.

Backup progress window

Backup operations for some computers can be lengthy. As an administrative aid, System Platform displays a window to report progress information during a backup operation.

Backup progress monitoring

The backup progress window shows:

- Time-stamped progress messages from System Platform and applications running on local template virtual computers. This includes messages filtered directly from backup logs, for example, data set backup start, pause, end, or failure.
- A backup process countdown timer. The timer counts down until the operation ends successfully, halts because of errors or manual termination, or the estimated timer value expires. The countdown timer supplements the progress message content. Thus users can make a more informed decision about whether a problem occurred requiring a system recovery.

Backup progress monitoring runs automatically for the following operations:

- Manual backup
- Template upgrade backup

Backup progress warning and error messages

The progress window indicates whether a warning or error condition originated in System Platform or in a specific template computer, including:

- *Non-fatal warning* messages, such as:
  - A message reporting a normal event that requires no remedial action.
  - A message reporting a failure to back up a data set that is nonexistent.
  - An unusually delayed series of progress messages on a particular template virtual computer suggests that the backup operation for that data set has a problem. In this case, choose either to continue the operation, or manually end the operation.
- *Fatal warning messages*—In the event of any critical backup error, the operation in progress immediately ends with a message describing the failure.

Note:

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

- You must repeatedly end a backup operation manually.
- System Platform automatically ends a backup operation because of system errors.

To aid in troubleshooting a failed system backup, you can get progress messages during the last backup from the Web Console Backup page.

Installing System Platform

Before you begin

Log on to the System Platform web console.

Procedure

1. Download the System Platform Release 6.3.7.0.05001 software from the Avaya Support website at http://support.avaya.com.

2. On the server, install System Platform Release 6.3.7.0.05001. For instructions, see Installation methods.

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

Next steps

(Optional) If this System Platform release requires a patch, install the required System Platform patch. For the patch information, see **Required patch** column in the “Compatibility matrix for the System Manager and System Platform software versions”.

Related links

Installing patches on page 45
Compatibility matrix for the System Manager and System Platform software versions on page 22
Upgrading a System Platform server on page 121
Installation checklist for System Platform on page 55

Upgrading System Manager

Before you begin

Get the System Manager Release 6.3 software from the Avaya Support site at http://support.avaya.com.

Procedure

Upgrade the System Manager template to Release 6.3. For more information, see Upgrading the System Manager template.

Next steps

For any postinstall patches that you must apply, see System Manager 6.3 release notes on the Avaya Support site at http://support.avaya.com.

Related links

Upgrading the System Manager template on page 143

Installing the System Manager Release 6.3.18 bin file

Before you begin

- Log on to the System Platform web console.
- Download the `System_Manager_6.3.18_r5505487.bin` file from the Avaya support website at http://support.avaya.com.

  For more information, see Downloading patches.

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, select the `System_Manager_6.3.18_r5505487.bin` file.
4. On the Patch Detail page, click **Install**.
5. To verify that the patch installation is successful, on the System Manager web console, at the upper-right corner, click the settings icon () and click **About**.
6. Click **Commit**.

Next steps

To get the updated kernel that is running in the memory, restart System Manager

Related links

Installing patches on page 45
Downloading patches on page 43

Chapter 10: Upgrading from System Manager 6.1 SP1.1, SP2, SP3, SP4, SP5, SP6, SP7, or SP8 on the same server

Introduction

This section describes the procedure to upgrade System Manager from Release 6.1 SP1.1, SP2, SP3, SP4, SP5, SP6, SP7, or SP8 to System Manager Release 6.3.18.

In this upgrade procedure, reuse the existing server, upgrade System Platform to Release 6.3.7.0.05001, upgrade the System Manager to Release 6.3, and install the `System_Manager_6.3.18_r5505487.bin` file.

Verifying the current software version

About this task

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

Procedure

1. Log on to the System Manager web console.
2. To view the build number, in the upper-right corner of the web console, click the **About** link.

   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 links

System Manager and System Platform patches on page 20
Compatibility matrix for the System Manager and System Platform software versions on page 22

Installing the System Platform patch

Procedure

1. Download the 6.0.2.6.5 patch for System Platform from the Avaya Support website at http://support.avaya.com. For instructions to download the patch, see Downloading patches.
2. Install the 6.0.2.6.5 patch on System Platform Release 6.0.2.0.5. For instructions, see Installing patches.

Related links

Downloading patches on page 43
Installing patches on page 45

Creating a backup of the System Manager data

Procedure

1. Log on to the System Platform web console.
2. From the System Platform web console, create a backup of the System Manager data. For instructions, see Creating a backup of the System Manager data through System Platform.

Related links

Creating a backup of the System Manager data through System Platform on page 46

Upgrading System Platform

Before you begin

- Log on to the System Platform Web Console.
- Obtain the System Platform 6.0.3.0.3 software from the PLDS website. For instructions to download the software, see Downloading patches on page 43.

Procedure

Upgrade System Platform to Release 6.0.3.0.3. For instructions, see Upgrading a server on page 121.

Related links

Downloading patches on page 43
Upgrading a System Platform server on page 121

Installing the System Platform patch

Procedure

1. Download the 6.0.3.9.3 patch for System Platform from the Avaya Support website at http://support.avaya.com. For instructions to download the patch, see Downloading patches.
2. Install the 6.0.3.9.3 patch on System Platform Release 6.0.3.0.3. For instructions, see Installing patches.

Related links

Downloading patches on page 43
Installing patches on page 45

Upgrade tasks

Installing the software patch for System Manager

Before you begin

Start an SSH session.

Procedure

1. Download the patch, `System_Manager_06_01_patch.sh`, for System Manager from the Avaya Support website at http://support.avaya.com.

   For instructions to download the patch, see Downloading patches.
2. Using the command line interface, install the patch for System Manager.

   For instructions, see Installing the System Manager patch using the command line interface.

Related links

Downloading patches on page 43
Installing the System Manager patch using the command line interface on page 44

Creating a backup of the System Manager data

Procedure

1. Log on to the System Platform web console.

2. From the System Platform web console, create a backup of the System Manager data. For instructions, see Creating a backup of the System Manager data through System Platform.

Related links

Creating a backup of the System Manager data through System Platform on page 46

Upgrading System Platform

Procedure

1. Get the System Platform 6.3.7.0.05001 software from the PLDS website at https://plds.avaya.com.

   For instructions to download the software, see Downloading patches

2. Upgrade System Platform 6.0.3.9.3 to Release 6.3.7.0.05001.

   For instructions, see Upgrading the System Platform server.

Related links

Downloading patches on page 43
Upgrading a System Platform server on page 121

Upgrading System Manager

Before you begin

Get the System Manager Release 6.3 software from the Avaya Support site at http://support.avaya.com.

Procedure

Upgrade the System Manager template to Release 6.3. For more information, see Upgrading the System Manager template.

Next steps

For any postinstall patches that you must apply, see System Manager 6.3 release notes on the Avaya Support site at http://support.avaya.com.

Related links

Upgrading the System Manager template on page 143

Installing the System Manager Release 6.3.18 bin file

Before you begin

- Log on to the System Platform web console.
- Download the `System_Manager_6.3.18_r5505487.bin` file from the Avaya support website at http://support.avaya.com.

  For more information, see Downloading patches.

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, select the `System_Manager_6.3.18_r5505487.bin` file.
4. On the Patch Detail page, click **Install**.
5. To verify that the patch installation is successful, on the System Manager web console, at the upper-right corner, click the settings icon () and click **About**.
6. Click **Commit**.

Next steps

To get the updated kernel that is running in the memory, restart System Manager

Related links

Installing patches on page 45
Downloading patches on page 43

Chapter 11: Upgrading from System Manager 6.1 SP1.1, SP2, SP3, SP4, SP5, or SP6, SP7, or SP8 on a new server

Introduction

This section describes the procedure to upgrade System Manager from Release 6.1 SP 1.1, SP2, SP3, SP4, SP5, SP6, SP7, or SP8 to Release 6.3.18.

In this upgrade procedure, replace the server with an HP DL360 G8 or a Dell R620 Server. On the new server, install System Platform Release 6.3.7.0.05001, the System Manager Release 6.3 template, and the `System_Manager_6.3.18_r5505487.bin` file.

Verifying the current software version

About this task

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

Procedure

1. Log on to the System Manager web console.
2. To view the build number, in the upper-right corner of the web console, click the **About** link.

   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 links

System Manager and System Platform patches on page 20
Compatibility matrix for the System Manager and System Platform software versions on page 22

Creating a backup of the System Manager data

Procedure

1. Log on to the System Platform web console.
2. From the System Platform web console, create a backup of the System Manager data. For instructions, see Creating a backup of the System Manager data through System Platform.

Related links

Creating a backup of the System Manager data through System Platform on page 46

Shutting down the System Platform Server

About this task

When you reboot or shut down the System Platform server, the system reboots or shuts down all the virtual machines running on System Platform. This can result in a service disruption.

Note:

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

Procedure

1. Click **Server Management** > **Server Reboot/Shutdown**.
2. On the Server Reboot/Shutdown page, click **Shutdown Server**.

Upgrade tasks on a new server

Installing System Platform

Before you begin

Log on to the System Platform web console.

Procedure

1. Download the System Platform release that is compatible with the current System Manager release from the Avaya Support website at http://support.avaya.com.
2. On the server, install the System Platform software.

   For instructions, see Installation methods. The network configuration for System Platform must be the same as the network configuration of System Manager.

Next steps

(Optional) If this System Platform release requires a patch, install the patch. For the patch information, see System Manager release notes for the specific release on the Avaya Support website at http://support.avaya.com.

Installing System Manager 6.1 SP1.1, SP2, SP3, SP4, SP5, SP6, SP7, or SP8

Before you begin

- Log on to the System Platform web console.
- Get the software for System Manager SP1.1, SP2, SP3, SP4, SP5, SP6, SP7, or SP8 from the PLDS website at https://plds.avaya.com.

Procedure

On the new server, install System Manager Release 6.1 SP1.1, SP2, SP3, SP4, SP5, SP6, SP7, or SP8.

For instructions, see *Installing and upgrading Avaya Aura® System Manager*, for the appropriate release. To download the documentation, see Downloading the documentation from the Avaya Support site.

Related links

Downloading patches on page 43
Downloading the documentation from the Avaya Support site on page 270

Installing the software patch for System Manager

Before you begin

Start an SSH session.

Procedure

1. Download the patch, `System_Manager_06_01_patch.sh`, for System Manager from the Avaya Support website at http://support.avaya.com.

   For instructions to download the patch, see Downloading patches.

2. Using the command line interface, install the patch for System Manager.

   For instructions, see Installing the System Manager patch using the command line interface.

Related links

Downloading patches on page 43
Installing the System Manager patch using the command line interface on page 44

Restoring the System Manager backup data

Before you begin

Log on to System Platform Web Console.

About this task

You can restore the backup data from System Manager that is configured for Geographic Redundancy on a standalone System Manager. However, you cannot restore the backup data from a standalone System Manager on System Manager that is configured for Geographic Redundancy.

You cannot restore the backup data on the primary System Manager server when the Geographic Redundancy replication is enabled on System Manager.

Note:

The restore operation does not restore the High Availability Failover configuration from the backup file. The restore feature does not reenable a failed High Availability Failover node back to High Availability Failover configuration. Follow the instructions given in this document on how to reenable a failed High Availability Failover node back to High Availability Failover configuration. Restore the backup configuration before configuring and starting High Availability Failover.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Restore**.
3. On the **Restore** tab, in the **Restore From** field, click `SFTP`.
4. Enter the details of the remote server on which the archive file is located:
   - **SFTP Hostname/IP**
   - **SFTP Directory**
   - **SFTP Username**
   - **SFTP Password**
5. Click **Search**.

   The system searches for archive files in the specified directory of the remote server.
6. To restore from the selected archive, select an archive file from the list, and then click **Restore**.

   The system displays the restore progress window in the Restore tab and displays restore event messages with timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - A system error condition abruptly halts the operation. In this case, contact Avaya Support at http://support.avaya.com.

When the restore progress window displays a message indicating successful completion of the operation, the system restarts. You must log on again to the System Platform web console.

Result

After the restore is complete on System Manager that is configured for Geographic Redundancy, the system automatically restarts with the Geographic Redundancy replication status as disabled.

Installing System Platform

Before you begin

Log on to the System Platform web console.

Procedure

1. Download the System Platform Release 6.3.7.0.05001 software from the Avaya Support website at http://support.avaya.com.
2. On the server, install System Platform Release 6.3.7.0.05001. For instructions, see Installation methods.

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

Next steps

(Optional) If this System Platform release requires a patch, install the required System Platform patch. For the patch information, see **Required patch** column in the “Compatibility matrix for the System Manager and System Platform software versions”.

Related links

Installing patches on page 45
Compatibility matrix for the System Manager and System Platform software versions on page 22
Upgrading a System Platform server on page 121
Installation checklist for System Platform on page 55

Upgrading System Manager

Before you begin

Get the System Manager Release 6.3 software from the Avaya Support site at http://support.avaya.com.

Procedure

Upgrade the System Manager template to Release 6.3. For more information, see Upgrading the System Manager template.

Next steps

For any postinstall patches that you must apply, see System Manager 6.3 release notes on the Avaya Support site at http://support.avaya.com.

Related links

Upgrading the System Manager template on page 143

Installing the System Manager Release 6.3.18 bin file

Before you begin

- Log on to the System Platform web console.
- Download the `System_Manager_6.3.18_r5505487.bin` file from the Avaya support website at http://support.avaya.com.

  For more information, see Downloading patches.

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, select the `System_Manager_6.3.18_r5505487.bin` file.
4. On the Patch Detail page, click **Install**.
5. To verify that the patch installation is successful, on the System Manager web console, at the upper-right corner, click the settings icon () and click **About**.
6. Click **Commit**.

Next steps

To get the updated kernel that is running in the memory, restart System Manager

Related links

Installing patches on page 45
Downloading patches on page 43

Chapter 12: Upgrading from System Manager 6.1 on the same server

Introduction

This section describes the procedure to upgrade System Manager from Release 6.1 running System Platform to Release 6.3.18.

In this upgrade procedure, reuse the existing server, upgrade System Platform to Release 6.3.7.0.05001, upgrade the System Manager to Release 6.3, and install the `System_Manager_6.3.18_r5505487.bin` file.

Note:

For instructions to upgrade System Manager from 6.1 SP1.1, SP2, SP3, SP4, SP5, SP6, SP7, or SP8 to Release 6.3.18, see Introduction on page 193.

Verifying the current software version

About this task

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

Procedure

1. Log on to the System Manager web console.
2. To view the build number, in the upper-right corner of the web console, click the **About** link.

   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 links

System Manager and System Platform patches on page 20
Compatibility matrix for the System Manager and System Platform software versions on page 22

Installing the System Platform patch

Procedure

1. Download the 6.0.2.6.5 patch for System Platform from the Avaya Support website at http://support.avaya.com. For instructions to download the patch, see Downloading patches.
2. Install the 6.0.2.6.5 patch on System Platform Release 6.0.2.0.5. For instructions, see Installing patches.

Related links

Downloading patches on page 43
Installing patches on page 45

Creating a backup of the System Manager data

Procedure

1. Log on to the System Platform web console.
2. From the System Platform web console, create a backup of the System Manager data. For instructions, see Creating a backup of the System Manager data through System Platform.

Related links

Creating a backup of the System Manager data through System Platform on page 46

Upgrading System Platform

Before you begin

- Log on to the System Platform Web Console.
- Obtain the System Platform 6.0.3.0.3 software from the PLDS website. For instructions to download the software, see Downloading patches on page 43.

Procedure

Upgrade System Platform to Release 6.0.3.0.3. For instructions, see Upgrading a server on page 121.

Related links

Downloading patches on page 43
Upgrading a System Platform server on page 121

Installing the System Platform patch

Procedure

1. Download the 6.0.3.9.3 patch for System Platform from the Avaya Support website at http://support.avaya.com. For instructions to download the patch, see Downloading patches.
2. Install the 6.0.3.9.3 patch on System Platform Release 6.0.3.0.3. For instructions, see Installing patches.

Related links

Downloading patches on page 43
Installing patches on page 45

Upgrade tasks

Installing the software patch for System Manager

Before you begin

Start an SSH session.

Procedure

1. Download the patch, `System_Manager_06_01_SP0_r873.bin`, for System Manager from the Avaya Support website at http://support.avaya.com.

   For instructions to download the patch, see Downloading patches.
2. Using the command line interface, install the patch for System Manager.

   For instructions, see Installing the System Manager patch using the command line interface.

Related links

Downloading patches on page 43
Installing the System Manager patch using the command line interface on page 44

Installing the software patch for System Manager

Before you begin

Start an SSH session.

Procedure

1. Download the patch, `System_Manager_06_01_patch.sh`, for System Manager from the Avaya Support website at http://support.avaya.com.

   For instructions to download the patch, see Downloading patches.

2. Using the command line interface, install the patch for System Manager.

   For instructions, see Installing the System Manager patch using the command line interface.

Related links

Downloading patches on page 43
Installing the System Manager patch using the command line interface on page 44

Creating a backup of the System Manager data

Procedure

1. Log on to the System Platform web console.
2. From the System Platform web console, create a backup of the System Manager data. For instructions, see Creating a backup of the System Manager data through System Platform.

Related links

Creating a backup of the System Manager data through System Platform on page 46

Upgrading System Platform

Procedure

1. Get the System Platform 6.3.7.0.05001 software from the PLDS website at https://plds.avaya.com.

   For instructions to download the software, see Downloading patches

2. Upgrade System Platform 6.0.3.9.3 to Release 6.3.7.0.05001.

   For instructions, see Upgrading the System Platform server.

Related links

Downloading patches on page 43
Upgrading a System Platform server on page 121

Upgrading System Manager

Before you begin

Get the System Manager Release 6.3 software from the Avaya Support site at http://support.avaya.com.

Procedure

Upgrade the System Manager template to Release 6.3. For more information, see Upgrading the System Manager template.

Next steps

For any postinstall patches that you must apply, see System Manager 6.3 release notes on the Avaya Support site at http://support.avaya.com.

Related links

Upgrading the System Manager template on page 143

Installing the System Manager Release 6.3.18 bin file

Before you begin

- Log on to the System Platform web console.
- Download the `System_Manager_6.3.18_r5505487.bin` file from the Avaya support website at http://support.avaya.com.

  For more information, see Downloading patches.

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, select the `System_Manager_6.3.18_r5505487.bin` file.
4. On the Patch Detail page, click **Install**.
5. To verify that the patch installation is successful, on the System Manager web console, at the upper-right corner, click the settings icon () and click **About**.
6. Click **Commit**.

Next steps

To get the updated kernel that is running in the memory, restart System Manager

Related links

Installing patches on page 45

Downloading patches on page 43

Chapter 13: Upgrading from System Manager 6.1 on a new server

Introduction

This section describes the procedure to upgrade System Manager from Release 6.1 to Release 6.3.18.

In this upgrade procedure, replace the server with an HP DL360 G8 or a Dell R620 Server. On the new server, install System Platform Release 6.3.7.0.05001, the System Manager Release 6.3 template, and the `System_Manager_6.3.18_r5505487.bin` file.

Note:

For instructions to upgrade System Manager from 6.1 SP1.1, SP2, SP3, SP4, SP5, SP6, SP7, or SP8 to Release 6.3.18, see Introduction on page 198.

Verifying the current software version

About this task

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

Procedure

1. Log on to the System Manager web console.
2. To view the build number, in the upper-right corner of the web console, click the **About** link.

   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 links

System Manager and System Platform patches on page 20
Compatibility matrix for the System Manager and System Platform software versions on page 22

Creating a backup of the System Manager data

Procedure

1. Log on to the System Platform web console.
2. From the System Platform web console, create a backup of the System Manager data. For instructions, see Creating a backup of the System Manager data through System Platform.

Related links

Creating a backup of the System Manager data through System Platform on page 46

Installing the software patch for System Manager

Before you begin

Start an SSH session.

Procedure

1. Download the patch, `System_Manager_06_01_SP0_r873.bin`, for System Manager from the Avaya Support website at http://support.avaya.com.

   For instructions to download the patch, see Downloading patches.

2. Using the command line interface, install the patch for System Manager.

   For instructions, see Installing the System Manager patch using the command line interface.

Related links

Downloading patches on page 43
Installing the System Manager patch using the command line interface on page 44

Creating a backup of the System Manager data

Procedure

1. Log on to the System Platform web console.
2. From the System Platform web console, create a backup of the System Manager data. For instructions, see Creating a backup of the System Manager data through System Platform.

Related links

Creating a backup of the System Manager data through System Platform on page 46

Shutting down the System Platform Server

About this task

When you reboot or shut down the System Platform server, the system reboots or shuts down all the virtual machines running on System Platform. This can result in a service disruption.

Note:

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

Procedure

1. Click **Server Management** > **Server Reboot/Shutdown**.
2. On the Server Reboot/Shutdown page, click **Shutdown Server**.

Upgrade tasks on a new server

Installing System Platform

Before you begin

Log on to the System Platform web console.

Procedure

1. Download the System Platform release that is compatible with the current System Manager release from the Avaya Support website at http://support.avaya.com.
2. On the server, install the System Platform software.

   For instructions, see Installation methods. The network configuration for System Platform must be the same as the network configuration of System Manager.

Next steps

(Optional) If this System Platform release requires a patch, install the patch. For the patch information, see System Manager release notes for the specific release on the Avaya Support website at http://support.avaya.com.

Installing System Manager 6.1

Before you begin

- Log on to System Platform Web Console.
- Obtain the software for System Manager 6.1 from the PLDS website at https://plds.avaya.com.

Procedure

On the new server, install the System Manager Release 6.1 template.

For instructions, see *Installing and upgrading Avaya Aura® System Manager*, for the appropriate release. To download the documentation, see Downloading the documentation from the Avaya Support site.

Related links

Downloading the documentation from the Avaya Support site on page 270

Installing the software patch for System Manager

Before you begin

Start an SSH session.

Procedure

1. Download the patch, `System_Manager_06_01_SP0_r873.bin`, for System Manager from the Avaya Support website at http://support.avaya.com.

   For instructions to download the patch, see Downloading patches.

2. Using the command line interface, install the patch for System Manager.

   For instructions, see Installing the System Manager patch using the command line interface.

Related links

Downloading patches on page 43
Installing the System Manager patch using the command line interface on page 44

Restoring the System Manager backup data

Before you begin

Log on to System Platform Web Console.

About this task

You can restore the backup data from System Manager that is configured for Geographic Redundancy on a standalone System Manager. However, you cannot restore the backup data from a standalone System Manager on System Manager that is configured for Geographic Redundancy.

You cannot restore the backup data on the primary System Manager server when the Geographic Redundancy replication is enabled on System Manager.

Note:

The restore operation does not restore the High Availability Failover configuration from the backup file. The restore feature does not reenable a failed High Availability Failover node back to High Availability Failover configuration. Follow the instructions given in this document on how

to reenable a failed High Availability Failover node back to High Availability Failover configuration. Restore the backup configuration before configuring and starting High Availability Failover.

Procedure

1. Click **Server Management** > **Backup/Restore**.
2. Click **Restore**.
3. On the **Restore** tab, in the **Restore From** field, click `SFTP`.
4. Enter the details of the remote server on which the archive file is located:
   - **SFTP Hostname/IP**
   - **SFTP Directory**
   - **SFTP Username**
   - **SFTP Password**
5. Click **Search**.

   The system searches for archive files in the specified directory of the remote server.
6. To restore from the selected archive, select an archive file from the list, and then click **Restore**.

   The system displays the restore progress window in the Restore tab and displays restore event messages with timestamps. The window remains open until any of the following events occur:

   - The operation concludes successfully.
   - A system error condition abruptly halts the operation. In this case, contact Avaya Support at http://support.avaya.com.

   When the restore progress window displays a message indicating successful completion of the operation, the system restarts. You must log on again to the System Platform web console.

Result

After the restore is complete on System Manager that is configured for Geographic Redundancy, the system automatically restarts with the Geographic Redundancy replication status as disabled.

Installing the software patch for System Manager

Before you begin

Start an SSH session.

Procedure

1. Download the patch, `System_Manager_06_01_patch.sh`, for System Manager from the Avaya Support website at http://support.avaya.com.

For instructions to download the patch, see Downloading patches.

2. Using the command line interface, install the patch for System Manager.

   For instructions, see Installing the System Manager patch using the command line interface.

Related links

Downloading patches on page 43
Installing the System Manager patch using the command line interface on page 44

Installing System Platform

Before you begin

Log on to the System Platform web console.

Procedure

1. Download the System Platform Release 6.3.7.0.05001 software from the Avaya Support website at http://support.avaya.com.
2. On the server, install System Platform Release 6.3.7.0.05001. For instructions, see Installation methods.

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

Next steps

(Optional) If this System Platform release requires a patch, install the required System Platform patch. For the patch information, see **Required patch** column in the “Compatibility matrix for the System Manager and System Platform software versions”.

Related links

Installing patches on page 45
Compatibility matrix for the System Manager and System Platform software versions on page 22
Upgrading a System Platform server on page 121
Installation checklist for System Platform on page 55

Upgrading System Manager

Before you begin

Get the System Manager Release 6.3 software from the Avaya Support site at http://support.avaya.com.

Procedure

Upgrade the System Manager template to Release 6.3. For more information, see Upgrading the System Manager template.

Next steps

For any postinstall patches that you must apply, see System Manager 6.3 release notes on the Avaya Support site at http://support.avaya.com.

Related links

Upgrading the System Manager template on page 143

Installing the System Manager Release 6.3.18 bin file

Before you begin

- Log on to the System Platform web console.
- Download the `System_Manager_6.3.18_r5505487.bin` file from the Avaya support website at http://support.avaya.com.

  For more information, see Downloading patches.

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, select the `System_Manager_6.3.18_r5505487.bin` file.
4. On the Patch Detail page, click **Install**.
5. To verify that the patch installation is successful, on the System Manager web console, at the upper-right corner, click the settings icon () and click **About**.
6. Click **Commit**.

Next steps

To get the updated kernel that is running in the memory, restart System Manager

Related links

Installing patches on page 45
Downloading patches on page 43

Chapter 14: Upgrading from System Manager 6.0 SP1 or SP2 on the same server

Introduction

This section describes the procedure to upgrade System Manager from Release 6.0 SP1 or 6.0 SP2 running on System Platform to Release 6.3.18.

In this upgrade procedure, reuse the existing server, upgrade System Platform to Release 6.3.7.0.05001, upgrade the System Manager to Release 6.3, and install the `System_Manager_6.3.18_r5505487.bin` file.

Verifying the current software version

About this task

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

Procedure

1. Log on to the System Manager web console.
2. To view the build number, in the upper-right corner of the web console, click the **About** link.

   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 links

System Manager and System Platform patches on page 20
Compatibility matrix for the System Manager and System Platform software versions on page 22

Installing the System Platform patch

Procedure

1. From the PLDS website at https://plds.avaya.com, download the following System Platform software:
   - For System Manager 6.0 SP1, the 6.0.0.3.11 patch.
   - For System Manager 6.0 SP2, the 6.0.2.6.5 patch.

   For instructions to download the software, see Downloading patches.
2. Install one of the following System Platform patch:
   - For System Manager 6.0 SP1, the 6.0.0.3.11 patch on System Platform Release 6.0.0.0.11.
   - For System Manager 6.0 SP2, the 6.0.2.6.5 patch on System Platform Release 6.0.2.0.5.

   For instructions, see Installing patches.

Related links

Installing patches on page 45
Downloading patches on page 43

Upgrade tasks

Creating a backup of the System Manager data

Before you begin

Log on to the System Manager web console.

Procedure

Create a backup of the System Manager data. For instructions, see Creating a data backup on a remote server.

Related links

Creating a data backup on a remote server on page 49

Upgrading System Platform

Before you begin

- Log on to the System Platform Web Console.

- Obtain the System Platform 6.0.3.0.3 software from the PLDS website. For instructions to download the software, see Downloading patches on page 43.

Procedure

Upgrade System Platform to Release 6.0.3.0.3. For instructions, see Upgrading a server on page 121.

Related links

Downloading patches on page 43

Upgrading a System Platform server on page 121

Installing the System Platform patch

Procedure

1. Download the 6.0.3.9.3 patch for System Platform from the Avaya Support website at http://support.avaya.com. For instructions to download the patch, see Downloading patches.
2. Install the 6.0.3.9.3 patch on System Platform Release 6.0.3.0.3. For instructions, see Installing patches.

Related links

Downloading patches on page 43

Installing patches on page 45

Creating a backup of the System Manager data

Before you begin

Log on to the System Manager web console.

Procedure

Create a backup of the System Manager data. For instructions, see Creating a data backup on a remote server.

Related links

Creating a data backup on a remote server on page 49

Upgrading System Platform

Procedure

1. Get the System Platform 6.3.7.0.05001 software from the PLDS website at https://plds.avaya.com.

For instructions to download the software, see Downloading patches

2. Upgrade System Platform 6.0.3.9.3 to Release 6.3.7.0.05001.

   For instructions, see Upgrading the System Platform server.

Related links

Downloading patches on page 43
Upgrading a System Platform server on page 121

Upgrading System Manager

Before you begin

Get the System Manager Release 6.3 software from the Avaya Support site at http://support.avaya.com.

Procedure

Upgrade the System Manager template to Release 6.3. For more information, see Upgrading the System Manager template.

Next steps

For any postinstall patches that you must apply, see System Manager 6.3 release notes on the Avaya Support site at http://support.avaya.com.

Related links

Upgrading the System Manager template on page 143

Installing the System Manager Release 6.3.18 bin file

Before you begin

- Log on to the System Platform web console.
- Download the `System_Manager_6.3.18_r5505487.bin` file from the Avaya support website at http://support.avaya.com.

  For more information, see Downloading patches.

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, select the `System_Manager_6.3.18_r5505487.bin` file.

4. On the Patch Detail page, click **Install**.
5. To verify that the patch installation is successful, on the System Manager web console, at the upper-right corner, click the settings icon () and click **About**.
6. Click **Commit**.

Next steps

To get the updated kernel that is running in the memory, restart System Manager

Related links

Installing patches on page 45
Downloading patches on page 43

Chapter 15: Upgrading from System Manager 6.0 SP1 or SP2 on a new server

Introduction

This section describes the procedure to upgrade System Manager from Release 6.0 SP1 or SP2 to System Manager Release 6.3.18.

In this upgrade procedure, replace the server with an HP DL360 G8 or a Dell R620 Server. On the new server, install System Platform Release 6.3.7.0.05001, the System Manager Release 6.3 template, and the `System_Manager_6.3.18_r5505487.bin` file.

Verifying the current software version

About this task

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

Procedure

1. Log on to the System Manager web console.
2. To view the build number, in the upper-right corner of the web console, click the **About** link.

   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 links

System Manager and System Platform patches on page 20
Compatibility matrix for the System Manager and System Platform software versions on page 22

Creating a backup of the System Manager data

Before you begin

Log on to the System Manager web console.

Procedure

Create a backup of the System Manager data. For instructions, see Creating a data backup on a remote server.

Related links

Creating a data backup on a remote server on page 49

Shutting down the System Platform Server

About this task

When you reboot or shut down the System Platform server, the system reboots or shuts down all the virtual machines running on System Platform. This can result in a service disruption.

Note:

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

Procedure

1. Click **Server Management** > **Server Reboot/Shutdown**.
2. On the Server Reboot/Shutdown page, click **Shutdown Server**.

Upgrade tasks on a new server

Installing System Platform

Before you begin

Log on to the System Platform web console.

Procedure

1. Download the System Platform release that is compatible with the current System Manager release from the Avaya Support website at http://support.avaya.com.
2. On the server, install the System Platform software.

For instructions, see Installation methods. The network configuration for System Platform must be the same as the network configuration of System Manager.

Next steps

(Optional) If this System Platform release requires a patch, install the patch. For the patch information, see System Manager release notes for the specific release on the Avaya Support website at http://support.avaya.com.

Installing System Manager 6.0 SP1

On the new server, install System Manager Release 6.0 SP1.

For instructions, see *Installing and upgrading Avaya Aura® System Manager*, for the appropriate release. To download the documentation, see Downloading the documentation from the Avaya Support site.

Restoring a backup from a remote server

Before you begin

Log on to the System Manager web console.

About this task

After the restore is complete on System Manager that is configured for Geographic Redundancy, the system automatically restarts with the Geographic Redundancy replication status as disabled.

Procedure

1. In the left navigation pane, click **System Manager Data** > **Backup and Restore**.
2. On the Backup and Restore page, click **Restore**.
3. On the Restore page, click **Remote**.
4. Enter the details in the **Remote server IP**, **Remote server port**, **User name**, **Password** fields, and provide the name of the file that you want to restore.
5. Click **Restore**.

   After a successful restore operation, the system logs you out of the System Manager Web Console. To use the system, you must log in again.

Installing System Platform

Before you begin

Log on to the System Platform web console.

Procedure

1. Download the System Platform Release 6.3.7.0.05001 software from the Avaya Support website at http://support.avaya.com.
2. On the server, install System Platform Release 6.3.7.0.05001. For instructions, see Installation methods.

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

Next steps

(Optional) If this System Platform release requires a patch, install the required System Platform patch. For the patch information, see **Required patch** column in the “Compatibility matrix for the System Manager and System Platform software versions”.

Related links

Installing patches on page 45
Compatibility matrix for the System Manager and System Platform software versions on page 22
Upgrading a System Platform server on page 121
Installation checklist for System Platform on page 55

Upgrading System Manager

Before you begin

Get the System Manager Release 6.3 software from the Avaya Support site at http://support.avaya.com.

Procedure

Upgrade the System Manager template to Release 6.3. For more information, see Upgrading the System Manager template.

Next steps

For any postinstall patches that you must apply, see System Manager 6.3 release notes on the Avaya Support site at http://support.avaya.com.

Related links

Upgrading the System Manager template on page 143

Installing the System Manager Release 6.3.18 bin file

Before you begin

- Log on to the System Platform web console.
- Download the `System_Manager_6.3.18_r5505487.bin` file from the Avaya support website at http://support.avaya.com.

For more information, see Downloading patches.

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, select the `System_Manager_6.3.18_r5505487.bin` file.
4. On the Patch Detail page, click **Install**.
5. To verify that the patch installation is successful, on the System Manager web console, at the upper-right corner, click the settings icon () and click **About**.
6. Click **Commit**.

Next steps

To get the updated kernel that is running in the memory, restart System Manager

Related links

Installing patches on page 45
Downloading patches on page 43

Chapter 16: Upgrading from System Manager 6.0 on the same server

Introduction

This section describes the procedure to upgrade System Manager from Release 6.0 running System Platform to Release 6.3.18.

In this upgrade procedure, reuse the existing server, upgrade System Platform to Release 6.3.7.0.05001, upgrade the System Manager to Release 6.3, and install the `System_Manager_6.3.18_r5505487.bin` file.

Note:

For instructions to upgrade System Manager from 6.0 SP1 or SP2 to Release 6.3.18, see Introduction on page 217.

Verifying the current software version

About this task

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

Procedure

1. Log on to the System Manager web console.
2. To view the build number, in the upper-right corner of the web console, click the **About** link.

   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 links

System Manager and System Platform patches on page 20
Compatibility matrix for the System Manager and System Platform software versions on page 22

Installing the System Platform patch

Procedure

1. Download the 6.0.0.3.11 patch for System Platform from the Avaya Support website at http://support.avaya.com.

   For instructions to download the patch, see Downloading patches.

2. Install the 6.0.0.3.11 patch on System Platform Release 6.0.0.0.11.

   For instructions, see Installing patches.

Upgrade tasks

Creating a backup of the System Manager data

Before you begin

Log on to the System Manager web console.

Procedure

Create a backup of the System Manager data. For instructions, see Creating a data backup on a remote server.

Related links

Creating a data backup on a remote server on page 49

Upgrading System Platform

Before you begin

- Log on to the System Platform Web Console.
- Obtain the System Platform 6.0.3.0.3 software from the PLDS website. For instructions to download the software, see Downloading patches on page 43.

Procedure

Upgrade System Platform to Release 6.0.3.0.3. For instructions, see Upgrading a server on page 121.

Related links

Downloading patches on page 43

Upgrading a System Platform server on page 121

Installing the System Platform patch

Procedure

1. Download the 6.0.3.9.3 patch for System Platform from the Avaya Support website at http://support.avaya.com. For instructions to download the patch, see Downloading patches.
2. Install the 6.0.3.9.3 patch on System Platform Release 6.0.3.0.3. For instructions, see Installing patches.

Related links

Downloading patches on page 43
Installing patches on page 45

Creating a backup of the System Manager data

Before you begin

Log on to the System Manager web console.

Procedure

Create a backup of the System Manager data. For instructions, see Creating a data backup on a remote server.

Related links

Creating a data backup on a remote server on page 49

Upgrading System Manager to Release 6.0 SP1

Before you begin

Log on to System Platform Web Console.

Procedure

1. Obtain the software for System Manager Release 6.0 SP1 from the PLDS website at https://plds.avaya.com .
2. Upgrade System Manager to Release 6.0 SP1.

   For instructions, see *Installing and upgrading Avaya Aura® System Manager*, for the appropriate release. To download the documentation, see Downloading the documentation from the Avaya Support site.

Related links

Downloading the documentation from the Avaya Support site on page 270

Creating a backup of the System Manager data

Before you begin

Log on to the System Manager web console.

Procedure

Create a backup of the System Manager data. For instructions, see Creating a data backup on a remote server.

Related links

Creating a data backup on a remote server on page 49

Upgrading System Platform

Procedure

1. Get the System Platform 6.3.7.0.05001 software from the PLDS website at https://plds.avaya.com.

   For instructions to download the software, see Downloading patches

2. Upgrade System Platform 6.0.3.9.3 to Release 6.3.7.0.05001.

   For instructions, see Upgrading the System Platform server.

Related links

Downloading patches on page 43
Upgrading a System Platform server on page 121

Upgrading System Manager

Before you begin

Get the System Manager Release 6.3 software from the Avaya Support site at http://support.avaya.com.

Procedure

Upgrade the System Manager template to Release 6.3. For more information, see Upgrading the System Manager template.

Next steps

For any postinstall patches that you must apply, see System Manager 6.3 release notes on the Avaya Support site at http://support.avaya.com.

Related links

Upgrading the System Manager template on page 143

Installing the System Manager Release 6.3.18 bin file

Before you begin

- Log on to the System Platform web console.
- Download the `System_Manager_6.3.18_r5505487.bin` file from the Avaya support website at http://support.avaya.com.

  For more information, see Downloading patches.

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, select the `System_Manager_6.3.18_r5505487.bin` file.
4. On the Patch Detail page, click **Install**.
5. To verify that the patch installation is successful, on the System Manager web console, at the upper-right corner, click the settings icon ( ) and click **About**.
6. Click **Commit**.

Next steps

To get the updated kernel that is running in the memory, restart System Manager

Related links

Installing patches on page 45
Downloading patches on page 43

Chapter 17: Upgrading from System Manager 6.0 on a new server

Introduction

This section describes the procedure to upgrade System Manager from Release 6.0 to Release 6.3.18.

In this upgrade procedure, replace the server with an HP DL360 G8 or a Dell R620 Server. On the new server, install System Platform Release 6.3.7.0.05001, the System Manager Release 6.3 template, and the `System_Manager_6.3.18_r5505487.bin` file.

Note:

For instructions to upgrade System Manager from 6.0 SP1 or SP2 to Release 6.3.18, see Introduction on page 222.

Verifying the current software version

About this task

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

Procedure

1. Log on to the System Manager web console.
2. To view the build number, in the upper-right corner of the web console, click the **About** link.

   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 links

System Manager and System Platform patches on page 20
Compatibility matrix for the System Manager and System Platform software versions on page 22

Creating a backup of the System Manager data

Before you begin

Log on to the System Manager web console.

Procedure

Create a backup of the System Manager data. For instructions, see Creating a data backup on a remote server.

Related links

Creating a data backup on a remote server on page 49

Installing the software patch for System Manager

Before you begin

Start an SSH session.

Procedure

1. Download the following software patches for System Manager from the Avaya Support website at http://support.avaya.com.
   - `SystemManager_06_00_Patch_01.sh`
   - `SystemManager_06_00_Patch_02.sh`

   For instructions, see Downloading patches.
2. Using the command line interface, install the patch for System Manager.

   For instructions, see Installing the System Manager patch using the command line interface.

Related links

Downloading patches on page 43
Installing the System Manager patch using the command line interface on page 44

Creating a backup of the System Manager data

Before you begin

Log on to the System Manager web console.

Procedure

Create a backup of the System Manager data. For instructions, see Creating a data backup on a remote server.

Related links

Creating a data backup on a remote server on page 49

Shutting down the System Platform Server

About this task

When you reboot or shut down the System Platform server, the system reboots or shuts down all the virtual machines running on System Platform. This can result in a service disruption.

Note:

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

Procedure

1. Click **Server Management** > **Server Reboot/Shutdown**.
2. On the Server Reboot/Shutdown page, click **Shutdown Server**.

Upgrade tasks on a new server

Installing System Platform

Before you begin

Log on to the System Platform web console.

Procedure

1. Download the System Platform Release 6.3.7.0.05001 software from the Avaya Support website at http://support.avaya.com.
2. On the server, install System Platform Release 6.3.7.0.05001. For instructions, see Installation methods.

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

Next steps

(Optional) If this System Platform release requires a patch, install the required System Platform patch. For the patch information, see **Required patch** column in the “Compatibility matrix for the System Manager and System Platform software versions”.

Related links

Installing patches on page 45

Compatibility matrix for the System Manager and System Platform software versions on page 22
Upgrading a System Platform server on page 121
Installation checklist for System Platform on page 55

Installing System Manager 6.0

On the new server, install System Manager Release 6.0.

For instructions, see *Installing and upgrading Avaya Aura® System Manager*, for the appropriate release. To download the documentation, see Downloading the documentation from the Avaya Support site.

Installing the software patch for System Manager

Before you begin

Start an SSH session.

Procedure

1. Download the following software patches for System Manager from the Avaya Support website at http://support.avaya.com.
   - `SystemManager_06_00_Patch_01.sh`
   - `SystemManager_06_00_Patch_02.sh`

   For instructions, see Downloading patches.
2. Using the command line interface, install the patch for System Manager.

   For instructions, see Installing the System Manager patch using the command line interface.

Related links

Downloading patches on page 43
Installing the System Manager patch using the command line interface on page 44

Restoring a backup from a remote server

Before you begin

Log on to the System Manager web console.

About this task

After the restore is complete on System Manager that is configured for Geographic Redundancy, the system automatically restarts with the Geographic Redundancy replication status as disabled.

Procedure

1. In the left navigation pane, click **System Manager Data** > **Backup and Restore**.
2. On the Backup and Restore page, click **Restore**.
3. On the Restore page, click **Remote**.
4. Enter the details in the **Remote server IP**, **Remote server port**, **User name**, **Password** fields, and provide the name of the file that you want to restore.
5. Click **Restore**.

   After a successful restore operation, the system logs you out of the System Manager Web Console. To use the system, you must log in again.

Upgrading System Manager to Release 6.0 SP1

Before you begin

Log on to System Platform Web Console.

Procedure

1. Obtain the software for System Manager Release 6.0 SP1 from the PLDS website at https://plds.avaya.com .
2. Upgrade System Manager to Release 6.0 SP1.

   For instructions, see *Installing and upgrading Avaya Aura® System Manager*, for the appropriate release. To download the documentation, see Downloading the documentation from the Avaya Support site.

Related links

Downloading the documentation from the Avaya Support site on page 270

Creating a backup of the System Manager data

Before you begin

Log on to the System Manager web console.

Procedure

Create a backup of the System Manager data. For instructions, see Creating a data backup on a remote server.

Related links

Creating a data backup on a remote server on page 49

Installing the software patch for System Manager

Before you begin

Start an SSH session.

Procedure

1. Download the software patch for System Manager, `SystemManager_06_00_SP1_Patch_01.bin`, from the Avaya Support website at http://support.avaya.com.

   For instructions to download the patch, see Downloading patches.

2. Using the command line interface, install the patch for System Manager.

   For instructions, see Installing the System Manager patch using the command line interface.

Related links

Downloading patches on page 43
Installing the System Manager patch using the command line interface on page 44

Upgrading System Manager

Before you begin

Get the System Manager Release 6.3 software from the Avaya Support site at http://support.avaya.com.

Procedure

Upgrade the System Manager template to Release 6.3. For more information, see Upgrading the System Manager template.

Next steps

For any postinstall patches that you must apply, see System Manager 6.3 release notes on the Avaya Support site at http://support.avaya.com.

Related links

Upgrading the System Manager template on page 143

Installing the System Manager Release 6.3.18 bin file

Before you begin

- Log on to the System Platform web console.
- Download the `System_Manager_6.3.18_r5505487.bin` file from the Avaya support website at http://support.avaya.com.

For more information, see Downloading patches.

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, select the `System_Manager_6.3.18_r5505487.bin` file.
4. On the Patch Detail page, click **Install**.
5. To verify that the patch installation is successful, on the System Manager web console, at the upper-right corner, click the settings icon () and click **About**.
6. Click **Commit**.

Next steps

To get the updated kernel that is running in the memory, restart System Manager

Related links

Installing patches on page 45
Downloading patches on page 43

Chapter 18: Upgrading from System Manager 5.2 SP1 or SP2 on a new server

Introduction

This section describes the procedure to upgrade System Manager from Release 5.2 SP 1 or SP2 to System Manager Release 6.3.18.

In this upgrade procedure, replace the server with an HP DL360 G8 or a Dell R620 Server. On the new server, install System Platform Release 6.3.7.0.05001, the System Manager Release 6.3 template, and the `System_Manager_6.3.18_r5505487.bin` file.

For faster upgrades from System Manager Release 5.2.x to Release 6.3.18, you can import the NRP data. For instructions, see Data migration from System Manager 5.2.

Verifying the current software version on System Manager 5.2.x or earlier

Procedure

1. Log in to System Manager from the command line interface (CLI).
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 links

System Manager and System Platform patches on page 20
Compatibility matrix for the System Manager and System Platform software versions on page 22

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!!`

Shutting down the System Platform Server

About this task

When you reboot or shut down the System Platform server, the system reboots or shuts down all the virtual machines running on System Platform. This can result in a service disruption.

Note:

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

Procedure

1. Click **Server Management** > **Server Reboot/Shutdown**.
2. On the Server Reboot/Shutdown page, click **Shutdown Server**.

Upgrade tasks on a new server

Installing System Platform

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Download the software for System Platform 1.1.1.0.2 from the Avaya Support website at http://support.avaya.com.
2. On the new server, install System Platform Release 1.1.1.0.2.

   For instructions, see Installation methods on page 55.

Installing the System Platform patch

Before you begin

Log on to System Platform Web Console.

Procedure

1. Download the 1.1.1.97.2 patch for System Platform from the Avaya Support website at http://support.avaya.com.

   For instructions to download the patch, see Downloading patches.
2. Install the 1.1.1.97.2 patch on System Platform Release 1.1.1.0.2.

   For instructions, see Installing patches.

Installing System Manager Release 5.2 SP 1

Before you begin

- Log on to System Platform Web Console.
- Download the System Manager Release 5.2 SP1 software from the Avaya Support website at http://support.avaya.com.

Procedure

On the new server, install System Manager Release 5.2 SP1.

For instructions, see *Installing and upgrading Avaya Aura® System Manager*, for the appropriate release. To download the documentation, see Downloading the documentation from the Avaya Support site.

Related links

Downloading the documentation from the Avaya Support site on page 270
Installing System Manager Release 5.2 on page 250

Restoring a backup from a remote server

Procedure

1. On the System Manager Web Console, click **Settings** > **Backup and Restore**.
2. On the Backup and Restore page, click **Restore**.
3. On the Restore page, click **Remote**.
4. Enter the details in the **SCP server IP**, **SCP server port**, **User name**, **Password** fields, and the name of the file that you want to restore.
5. Click **Restore**.

   After the successful restore operation, the system logs you out of the System Manager Web Console. To use the system, you must log in again.

Upgrading System Platform

Before you begin

- Log on to the System Platform Web Console.
- Obtain the System Platform 6.0.2.0.5 software from the PLDS Web site at https://plds.avaya.com. For instructions to download the software, see Downloading patches on page 43.

Procedure

Upgrade System Platform 1.1.1.97.2 to Release 6.0.2.0.5. For instructions, see Upgrading a server on page 121.

Installing the System Platform patch

Procedure

1. Download the 6.0.2.6.5 patch for System Platform from the Avaya Support website at http://support.avaya.com. For instructions to download the patch, see Downloading patches.
2. Install the 6.0.2.6.5 patch on System Platform Release 6.0.2.0.5. For instructions, see Installing patches.

Related links

Downloading patches on page 43
Installing patches on page 45

Upgrading System Manager to Release 6.0 SP1

Before you begin

Log on to System Platform Web Console.

Procedure

1. Obtain the software for System Manager Release 6.0 SP1 from the PLDS website at https://plds.avaya.com .
2. Upgrade System Manager to Release 6.0 SP1.

   For instructions, see *Installing and upgrading Avaya Aura® System Manager*, for the appropriate release. To download the documentation, see Downloading the documentation from the Avaya Support site.

Related links

Downloading the documentation from the Avaya Support site on page 270

Creating a backup of the System Manager data

Before you begin

Log on to the System Manager web console.

Procedure

Create a backup of the System Manager data. For instructions, see Creating a data backup on a remote server.

Related links

Creating a data backup on a remote server on page 49

Installing the software patch for System Manager

Before you begin

Start an SSH session.

Procedure

1. Download the software patch for System Manager, `SystemManager_06_00_SP1_Patch_01.bin`, from the Avaya Support website at http://support.avaya.com.

   For instructions to download the patch, see Downloading patches.
2. Using the command line interface, install the patch for System Manager.

   For instructions, see Installing the System Manager patch using the command line interface.

Related links

Downloading patches on page 43
Installing the System Manager patch using the command line interface on page 44

Creating a backup of the System Manager data

Before you begin

Log on to the System Manager web console.

Procedure

Create a backup of the System Manager data. For instructions, see Creating a data backup on a remote server.

Related links

Creating a data backup on a remote server on page 49

Upgrading System Platform

Before you begin

- Log on to the System Platform Web Console.
- Obtain the System Platform 6.0.3.0.3 software from the PLDS website. For instructions to download the software, see Downloading patches on page 43.

Procedure

Upgrade System Platform to Release 6.0.3.0.3. For instructions, see Upgrading a server on page 121.

Related links

Downloading patches on page 43
Upgrading a System Platform server on page 121

Installing the System Platform patch

Procedure

1. Download the 6.0.3.9.3 patch for System Platform from the Avaya Support website at http://support.avaya.com. For instructions to download the patch, see Downloading patches.
2. Install the 6.0.3.9.3 patch on System Platform Release 6.0.3.0.3. For instructions, see Installing patches.

Related links

Downloading patches on page 43
Installing patches on page 45

Upgrading System Platform

Procedure

1. Get the System Platform 6.3.7.0.05001 software from the PLDS website at https://plds.avaya.com.

   For instructions to download the software, see Downloading patches

2. Upgrade System Platform 6.0.3.9.3 to Release 6.3.7.0.05001.

   For instructions, see Upgrading the System Platform server.

Related links

Downloading patches on page 43
Upgrading a System Platform server on page 121

Upgrading System Manager

Before you begin

Get the System Manager Release 6.3 software from the Avaya Support site at http://support.avaya.com.

Procedure

Upgrade the System Manager template to Release 6.3. For more information, see Upgrading the System Manager template.

Next steps

For any postinstall patches that you must apply, see System Manager 6.3 release notes on the Avaya Support site at http://support.avaya.com.

Related links

Upgrading the System Manager template on page 143

Installing the System Manager Release 6.3.18 bin file

Before you begin

- Log on to the System Platform web console.
- Download the `System_Manager_6.3.18_r5505487.bin` file from the Avaya support website at http://support.avaya.com.

  For more information, see Downloading patches.

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, select the `System_Manager_6.3.18_r5505487.bin` file.
4. On the Patch Detail page, click **Install**.
5. To verify that the patch installation is successful, on the System Manager web console, at the upper-right corner, click the settings icon () and click **About**.
6. Click **Commit**.

Next steps

To get the updated kernel that is running in the memory, restart System Manager

Related links

Installing patches on page 45
Downloading patches on page 43

Chapter 19: Upgrading from System Manager 5.2 on a new server

Introduction

This section describes the procedure to upgrade System Manager from Release 5.2 to Release 6.3.18.

In this upgrade procedure, replace the server with an HP DL360 G8 or a Dell R620 Server. On the new server, install System Platform Release 6.3.7.0.05001, the System Manager Release 6.3 template, and the `System_Manager_6.3.18_r5505487.bin` file.

Note:

For instructions to upgrade System Manager from 5.2 SP1 or SP2 to Release 6.3.18, see Introduction on page 239.

For faster upgrades from System Manager Release 5.2.x to Release 6.3.18, you can import the NRP data. For instructions, see Data migration from System Manager 5.2.

Verifying the current software version on System Manager 5.2.x or earlier

Procedure

1. Log in to System Manager from the command line interface (CLI).
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 links

System Manager and System Platform patches on page 20
Compatibility matrix for the System Manager and System Platform software versions on page 22

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!!`

Installing the software patch for System Manager

Before you begin

Start an SSH session.

Procedure

1. Download the software patch for System Manager, `System_Manager_05_02_GA_Patch_01.zip`, from the Avaya Support website at http://support.avaya.com.

   For instructions to download the patch, see Downloading patches.
2. Using the command line interface, install the patch for System Manager.

   For instructions, see Installing the System Manager patch using the command line interface.

Related links

Downloading patches on page 43
Installing the System Manager patch using the command line interface on page 44

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!!`

Shutting down the System Platform Server

About this task

When you reboot or shut down the System Platform server, the system reboots or shuts down all the virtual machines running on System Platform. This can result in a service disruption.

Note:

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

Procedure

1. Click **Server Management** > **Server Reboot/Shutdown**.
2. On the Server Reboot/Shutdown page, click **Shutdown Server**.

Upgrade tasks on a new server

Installing System Platform

Before you begin

Log on to the System Platform Web Console.

Procedure

1. Download the software for System Platform 1.1.1.0.2 from the Avaya Support website at http://support.avaya.com.
2. On the new server, install System Platform Release 1.1.1.0.2.

   For instructions, see Installation methods on page 55.

Installing the System Platform patch

Before you begin

Log on to System Platform Web Console.

Procedure

1. Download the 1.1.1.97.2 patch for System Platform from the Avaya Support website at http://support.avaya.com.

   For instructions to download the patch, see Downloading patches.
2. Install the 1.1.1.97.2 patch on System Platform Release 1.1.1.0.2.

   For instructions, see Installing patches.

Installing System Manager Release 5.2

Before you begin

- Log on to System Platform Web Console.
- Download System Manager Release 5.2 from the Avaya Support website at http://support.avaya.com.

Procedure

On the new server, install System Manager Release 5.2.

For instructions, see *Installing and upgrading Avaya Aura® System Manager*, for the appropriate release. To download the documentation, see Downloading the documentation from the Avaya Support site.

Related links

Downloading the documentation from the Avaya Support site on page 270

Installing the software patch for System Manager

Before you begin

Start an SSH session.

Procedure

1. Download the software patch for System Manager, `System_Manager_05_02_GA_Patch_01.zip`, from the Avaya Support website at http://support.avaya.com.

   For instructions to download the patch, see Downloading patches.

2. Using the command line interface, install the patch for System Manager.

   For instructions, see Installing the System Manager patch using the command line interface.

Related links

Downloading patches on page 43
Installing the System Manager patch using the command line interface on page 44

Restoring a backup from a remote server

Procedure

1. On the System Manager Web Console, click **Settings** > **Backup and Restore**.
2. On the Backup and Restore page, click **Restore**.
3. On the Restore page, click **Remote**.
4. Enter the details in the **SCP server IP**, **SCP server port**, **User name**, **Password** fields, and the name of the file that you want to restore.
5. Click **Restore**.

   After the successful restore operation, the system logs you out of the System Manager Web Console. To use the system, you must log in again.

Upgrading System Platform

Before you begin

- Log on to the System Platform Web Console.
- Obtain the System Platform 6.0.2.0.5 software from the PLDS Web site at https://plds.avaya.com. For instructions to download the software, see Downloading patches on page 43.

Procedure

Upgrade System Platform 1.1.1.97.2 to Release 6.0.2.0.5. For instructions, see Upgrading a server on page 121.

Installing the System Platform patch

Procedure

1. Download the 6.0.2.6.5 patch for System Platform from the Avaya Support website at http://support.avaya.com. For instructions to download the patch, see Downloading patches.
2. Install the 6.0.2.6.5 patch on System Platform Release 6.0.2.0.5. For instructions, see Installing patches.

Related links

Downloading patches on page 43
Installing patches on page 45

Upgrading System Manager to Release 6.0 SP1

Before you begin

Log on to System Platform Web Console.

Procedure

1. Obtain the software for System Manager Release 6.0 SP1 from the PLDS website at https://plds.avaya.com .
2. Upgrade System Manager to Release 6.0 SP1.

   For instructions, see *Installing and upgrading Avaya Aura® System Manager*, for the appropriate release. To download the documentation, see Downloading the documentation from the Avaya Support site.

Related links

Downloading the documentation from the Avaya Support site on page 270

Creating a backup of the System Manager data

Before you begin

Log on to the System Manager web console.

Procedure

Create a backup of the System Manager data. For instructions, see Creating a data backup on a remote server.

Related links

Creating a data backup on a remote server on page 49

Installing the software patch for System Manager

Before you begin

Start an SSH session.

Procedure

1. Download the software patch for System Manager, `SystemManager_06_00_SP1_Patch_01.bin`, from the Avaya Support website at http://support.avaya.com.

   For instructions to download the patch, see Downloading patches.

2. Using the command line interface, install the patch for System Manager.

   For instructions, see Installing the System Manager patch using the command line interface.

Related links

Downloading patches on page 43
Installing the System Manager patch using the command line interface on page 44

Creating a backup of the System Manager data

Before you begin

Log on to the System Manager web console.

Procedure

Create a backup of the System Manager data. For instructions, see Creating a data backup on a remote server.

Related links

Creating a data backup on a remote server on page 49

Upgrading System Platform

Before you begin

- Log on to the System Platform Web Console.
- Obtain the System Platform 6.0.3.0.3 software from the PLDS website. For instructions to download the software, see Downloading patches on page 43.

Procedure

Upgrade System Platform to Release 6.0.3.0.3. For instructions, see Upgrading a server on page 121.

Related links

Downloading patches on page 43

Upgrading a System Platform server on page 121

Installing the System Platform patch

Procedure

1. Download the 6.0.3.9.3 patch for System Platform from the Avaya Support website at http://support.avaya.com. For instructions to download the patch, see Downloading patches.
2. Install the 6.0.3.9.3 patch on System Platform Release 6.0.3.0.3. For instructions, see Installing patches.

Related links

Downloading patches on page 43
Installing patches on page 45

Upgrading System Platform

Procedure

1. Get the System Platform 6.3.7.0.05001 software from the PLDS website at https://plds.avaya.com.

   For instructions to download the software, see Downloading patches
2. Upgrade System Platform 6.0.3.9.3 to Release 6.3.7.0.05001.

   For instructions, see Upgrading the System Platform server.

Related links

Downloading patches on page 43
Upgrading a System Platform server on page 121

Upgrading System Manager

Before you begin

Get the System Manager Release 6.3 software from the Avaya Support site at http://support.avaya.com.

Procedure

Upgrade the System Manager template to Release 6.3. For more information, see Upgrading the System Manager template.

Next steps

For any postinstall patches that you must apply, see System Manager 6.3 release notes on the Avaya Support site at http://support.avaya.com.

Related links

Upgrading the System Manager template on page 143

Installing the System Manager Release 6.3.18 bin file

Before you begin

- Log on to the System Platform web console.
- Download the `System_Manager_6.3.18_r5505487.bin` file from the Avaya support website at http://support.avaya.com.

  For more information, see Downloading patches.

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, select the `System_Manager_6.3.18_r5505487.bin` file.
4. On the Patch Detail page, click **Install**.
5. To verify that the patch installation is successful, on the System Manager web console, at the upper-right corner, click the settings icon ( ) and click **About**.
6. Click **Commit**.

Next steps

To get the updated kernel that is running in the memory, restart System Manager

Related links

Installing patches on page 45
Downloading patches on page 43

Chapter 20: Upgrading System Manager 1.x

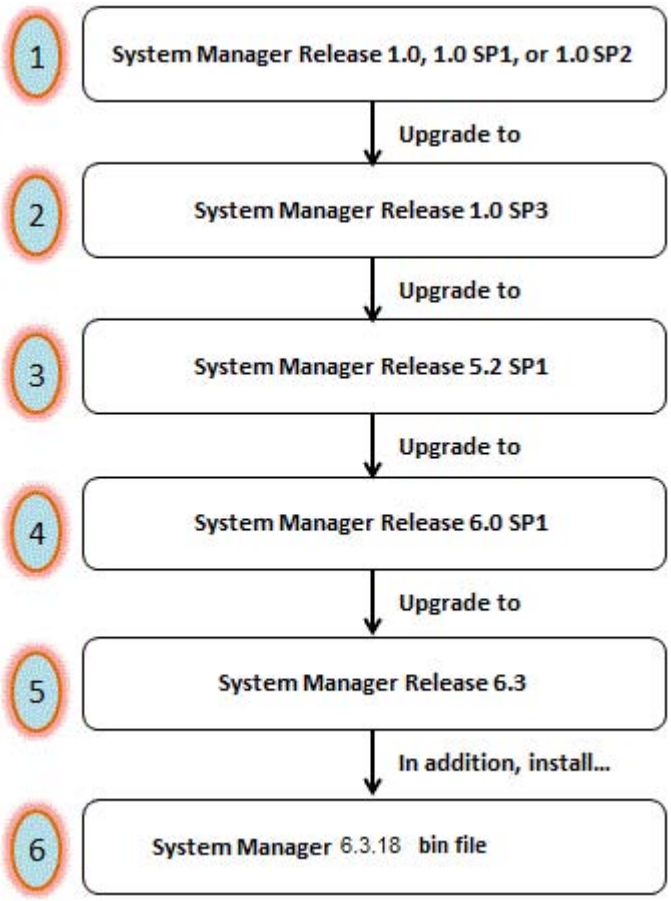
Upgrading from System Manager 1.x to Release 6.3.18

About this task

To upgrade System Manager from releases earlier than 1.0 SP3 to Release 6.3.18, you must perform multistep upgrades. You cannot directly upgrade to Release 6.3.18.

Perform the upgrades in the same sequence that is displayed in the image.

Procedure



Related links

Upgrading System Manager from 1.0 SP3 to 5.2 SP1 on page 257

Installing patches on page 45
Installation methods on page 55
Introduction on page 222

Upgrading System Manager from 1.0 SP3 to 5.2 SP1

Before you begin

- Create a backup of the System Manager 1.0 SP3 configuration data.

  For more information, see Creating a data backup on a remote server.
- Download the System Manager 5.2 SP1 template from the Avaya Support website at http://support.avaya.com.

Procedure

1. To create the `/opt/vsp` folder on the computer on which System Manager 1.0 SP3 is installed, at the command prompt, type `mkdir -p /opt/vsp`.
2. Copy the `BackupSMGR-R1xSP3.sh` and `vspUtil.jar` files that you downloaded from the Avaya Support website to the `/ opt/vsp` folder.
3. To convert the file to UNIX text file format, at the command prompt, type `dos2unix BackupSMGR-R1xSP3.sh`.
4. For permission to execute the script file, type `chmod +x BackupSMGR-R1xSP3.sh`.
5. To run the `BackupSMGR-R1xSP3.sh` script file, at the command prompt, type `sh BackupSMGR-R1xSP3.sh`.
6. If you are performing the upgrade process on the same computer, copy the `/tmp/MgmtBackup_1.0.*.zip` file to a different computer on the network.
7. Install System Platform Release 1.1.1.0.2.

   For instructions, see Installing System Platform.
8. Install the 1.1.1.97.2 patch on System Platform Release 1.1.1.0.2.

   For instructions, see Installing patches.
9. Install the System Manager template.

   For instructions, see *Installing and upgrading Avaya Aura® System Manager*, for the appropriate release. To download the documentation, see Downloading the documentation from the Avaya Support site.

   Note:

   In this upgrade process, the Hostname and IP Address, Domain Name, Gateway Address, Network Mask, and DNS must be the same as that of the computer on which you installed the System Manager 1.0 SP3 template. If you are using a different

computer for System Platform installation, shut down the computer on which System Manager 1.0 SP3 is running.

10. Copy the `MgmtBackup_1.0.*.zip` file to the `/ tmp/` folder on System Manager 5.2 SP1.
11. To run the `RestoreSMGR.sh` script file, navigate to the `/opt/vsp` folder and type `sh RestoreSMGR.sh`.

    The system upgrades System Manager from 1.0 SP3 to 5.2 SP1.

Next steps

- Upgrade System Manager 5.2 SP1 to System Manager 6.0 SP1. For instructions, see *Installing and Upgrading Avaya Aura® System Manager Release 6.1* available on the Avaya Support website at http://support.avaya.com.
- Upgrade System Manager 6.0 SP1 to System Manager Release 6.3. For instructions, see Upgrading System Manager 6.0 SP1 or SP2 on a new server.

Related links

Creating a data backup on a remote server on page 168

Chapter 21: Postupgrade verification

Verifying the functionality of System Manager

About this task

Note:

To ensure that System Manager is working correctly after the upgrade, verify that the installation of System Manager is successful.

When you upgrade to System Manager Release 6.3.18 from release:

- 6.0.x or 6.1.x. For 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 6.2 and later remain the same as in Release 6.1.
- 6.0.x. The system resets the admin password.
- 6.1.x or later. The admin password remains unchanged.

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

Procedure

1. Type `https://<fully qualified domain name of System Manager>/SMGR` on the web browser to log on to the System Manager web console of the upgraded system.
2. Click the settings icon (), click **About**, and verify that the system displays the version number of System Manager with the highest build number for the release.
3. To verify if the system has generated any new call processing alarms during the System Manager upgrade, perform the following:
   a. Click **Services** > **Events**.
   b. In the left navigation pane, click **Events** > **Alarms**.
   c. On the Alarms page, in the **Alarms List** section, note alarms that the system generated.

4. 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 information, see Managing users and Managing roles sections in *Administering Avaya Aura® System Manager*.
5. 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 by using Data Replication Service (DRS)

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

Chapter 22: Configuring System Manager

System Manager configuration

See Administering Avaya Aura® System Manager to complete the following administrative tasks:

- Set up Geographic Redundancy.
- Add Network Management Systems (NMS) Destination.
- Generate test alarms.
- Configure date and time.
- Backup and restore System Manager.

Network Management Systems Destinations

The Session Manager serviceability agent can send SNMPv2c/v3 traps or informs for alarms to multiple destinations such as:

- SAL Gateway (mandatory)
- System Manager Trap Listener
- Third-party NMS
- Avaya SIG server

SAL Gateway is a mandatory trap destination for traps sent to Avaya Services for system maintenance. SAL Gateway converts the traps to alarms and forwards the alarms to the Avaya Data Centre for ticketing purposes. Therefore, after you install or upgrade from release earlier than 6.2 to Session Manager Release 6.2 or later, you must configure the serviceability agent with the SAL Gateway as a trap destination. You can configure the serviceability agent by using System Manager Web Console. You must also configure Session Manager as a managed device on the SAL Gateway. Optionally, you can configure any third-party Network Management Systems (NMS) as a trap destination. Based on customer requirements, Avaya technicians can also configure Avaya SIG server as another trap destination.

For upgrades from Release 6.2 or later, the configuration of the serviceability agent persists through the Session Manager upgrade.

You can add an NMS destination using System Manager Web Console. To add an NMS destination, you must create a target profile for the NMS destination and then attach the target profile to a

serviceability agent. For more information on activating agents and attaching target profiles, see Managing Serviceability Agents in *Administering Avaya Aura® System Manager*.

Creating a data backup on a remote server

Procedure

1. On the 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:
     a. In the **File transfer protocol** field, click `SCP` or `SFTP`.
     b. Enter 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, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can 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 links

System Manager data backup options on page 49

Chapter 23: Changing over to Cold Standby server

Cold Standby server as failover server for System Manager

When the main server running System Manager fails, a cold standby System Manager server acts as a failover server.

This section covers the Cold Standby failover process for the System Manager application deployed on System Platform. This section explains the process with an example that has two nodes, one active and the other the cold standby node.

The section refers to Node A as the primary server that is active. Node B is the cold standby server. Execute the cold standby procedure with Node A going down and the application changed to Node B.

Prerequisites for the cold standby procedure

1. Ensure that the primary (Node A) and Cold Standby (Node B) servers are identical and have the same IP address and host name. When the primary server is running, the Standby server must be turned off.
2. Deploy the System Manager template on the primary and Standby server. For instructions, see *Implementing Avaya Aura® System Manager* installation.
3. Ensure that the system date is identical on both the servers.
4. Using the remote backup capability of System Manager Element Manager, create a regular backup of the System Manager database of the primary server to ensure that you have the latest data that you need for a cold standby procedure in case the primary server fails.

   Create the backup of the database on a remote computer or on an external storage device such as a Tape drive and DVD using System Platform. When the primary server fails, use the backup to restore the database on the standby server. For more information, see Creating a backup of the SMGR data through System Platform on page 46.

Implementing the cold standby procedure on another computer

About this task

When you implement the System Manager cold standby procedure on a different computer, the system does not recognize the previously installed license file as the MAC address changes for the new computer. Use the following workaround for this scenario:

Procedure

1. Generate a new license file for products that are licensed using WebLM and that were installed prior to performing cold standby. Ensure that this new license file is generated from PLDS with the same count and the new MAC address.
2. Copy the newly generated license file where System Manager is deployed.
3. Log in to the System Manager command line interface (CLI) and perform the following steps:
   a. To stop the JBoss server., enter `# service jboss stop`.
   b. Delete the unwanted license file with the file extension in XML from the `$JBOSS_HOME/server/avmgmt/deploy/WebLM.ear/WebLM.war/licenses` location.
   c. To find the license file that you must delete, open the license (.xml) file in a vi editor and search for the <Name> tag in the <Product> element.
   d. Verify that the name of the product is similar to the newly generated product name.
   e. Type `# rm -rf JBOSS_HOME/server/avmgmt/deploy/WebLM.ear/WebLM.war/licenses/<license file_name that is deleted>`.

      The system deletes the license file that you selected.
   f. To start the JBoss server, enter `# service jboss start`.

      Note:

      The system takes about 5 to 10 minutes to start the Jboss service.
4. Log on to the System Manager web console as `admin`.
5. Click **Services** > **Licenses** > **Install licenses**.
6. Click **Browse** and select the newly generated license file.
7. Click **Install**.
8. Verify that the system successfully installed the new license file.
9. Perform Step 1 through Step 10 for each product.

Setting up a Cold Standby server

Before you begin

Ensure that the primary server (Node A) is turned off.

Procedure

1. Turn on the standby server (Node B).
2. Install the System Manager patches on Node B that were installed on Node A before you took the last backup on Node A.

   For example, if you installed patch 1 and patch 2 on System Manager on Node A before the backup, then install patch 1 and patch 2 on Node B before you restore the backup. In case, patch 3 is available and not installed on Node A when the backup was taken, install only patch 1 and patch 2 on Node B. Do not install patch 3.
3. Restore the last database backup that you took from the Node A on Node B by using the backup and restore utility of System Manager Element Manager provided with System Manager. For more information, see Restoring a backup from a remote server on page 268.
4. After restoring the database on Node B, run the `postColdStandBy.sh` script on Node B from the location `@ $MGMT_HOME/utils/bin/coldstandby/postColdStandBy.sh`

   Note:

   After restoring and running the `postColdStandBy.sh` script, System Manager on Node B is available for operations.
5. After restoring the database on Node B, run the following steps to retrieve the TM truststore password:

   a. `sh /home/ucmdeploy/quantum/queryDefaultCertInfo.sh`

   b. Restart jboss.
6. After System Manager comes up, run repair on all the replica nodes to ensure the replicas have data that is consistent with the data restore on System Manager.
7. To repair the nodes: A, B, and C, perform the following steps:

   a. Log in to System Manager as an administrator.

   b. Click **Services** > **Replications** to open the replication page.

   c. Select all the replica groups and click **Repair**. The repair time of all the nodes depends on the number of nodes and the size of data populated in the System Manager database.

CLI restore for cold standby

CLI utility properties

You can use the cold standby procedure to restore the System Manager database using the CLI utility.

While restoring the System Manager data using the CLI, you might require to modify some of the restore properties related to the current setup. This `$MGMT_HOME/pem/fileRestoreCLIUtility/fileRestoreCLIUtility.properties` file contains the properties related to the CLI restore.

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

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

Table continues…

No	Property Name	Description
		value of the backup_name property must be /var/lib/pgsql/backup/manual/backup.zip.
10.	scp	The location of the backup archive. Specifies whether the backup archive is stored on the local computer on which System Manager is running or a remote computer. If the value is **false** it means the archive is on a local computer on which System Manager is running. If the value is **true** it means the archive is on a remote computer. The default is **false**.
11.	scp_ip	The IP or the host name of the remote server with the backup archive. Use this property when the scp value is **true**.
12.	scp_port	The ssh port used to connect to a remote server with a backup archive. The default is 22. Use this property when the scp value is set to **true**.
13.	user	The user performing the restore operation. You can specify any user name.
14.	remote_utility_directory	The full path to the directory that has the System Manager utilities required for the restore. The default is set to `/var/lib/pgsql`. Do not change the default setting.

Creating a data backup on a remote server

Procedure

1. On the 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:
     a. In the **File transfer protocol** field, click `SCP` or `SFTP`.
     b. Enter 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, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can 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 links

System Manager data backup options on page 49

Scheduling a data backup on a remote server

Procedure

1. On the 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:
   - Specify the SCP server IP, SCP server port, user name, password, and file name in the respective fields.
   - Select the **Use Default** check box.

     Important:

     To use the **Use Default** option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click **Services** > **Configurations**and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.
5. Click **Schedule**.
6. On the Schedule Backup page, specify the following details in the appropriate fields:
   - Job name
   - Date and time when the system must run the job
   - Frequency at which the system must run the job
   - Range
7. Click **Commit**.

Restoring a backup from a remote server

About this task

Note:

- Do not restore the backup data from VMware on System Platform.
- You cannot restore the backup data on the primary System Manager server when the Geographic Redundancy replication is enabled on System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Backup and Restore**.

2. On the Backup and Restore page, click **Restore**.
3. On the Restore page, click **Remote**.
4. In the **Parameterized Restore** tab, perform one of the following:
   - Provide the name of the file that you must restore, the file transfer protocol, the remote server IP, remote server port, user name, and the password to access the remote computer in the respective fields.

     Note:

     The backup integrity check feature of System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.

   - Select the **Use Default** check box.

     Important:

     To use the **Use Default** option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click **Services** > **Configurations**and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.
5. In the Backup List, view the list of the remote backups that are created by using the SFTP and SCP protocols.

   If the location of a backup file is modified, in the **Parameterized Restore** tab, specify the correct location of the backup file in the **File Name** field. You can select only one file at a time.
6. Click **Restore**. On the Restore Confirmation page, the system displays the following message:

   ```
   The Restore operation will terminate all sessions and no services
   will be available until the operation completes. So, the System
   Manager console will not be available for approximately 45 minutes
   but this time may vary based on Database size. Click on Continue to
   go ahead with the Restore operation or click on Cancel to abort the
   operation.
   ```
7. Click **Continue**.

   The system logs you out of the System Manager web console and then shuts down.

Result

After the restore is complete on System Manager that is configured for Geographic Redundancy, the system automatically restarts with the Geographic Redundancy replication status as disabled.

Appendix A: Downloading the documentation from the Avaya Support site

Procedure

1. On your Web browser, type `http://support.avaya.com`.
2. On the main menu, click **DOWNLOADS & DOCUMENTS**.
3. In the **Enter Your Product Here** field, enter `System Manager`.
4. In the **Select a content type** field, click `Documents` and click **Enter**.
5. In the Choose Release field, click the release number of the document that you want to view or download.
6. In the **Content Type** pane, select a check box for the content type you want to view or download.
7. From the list of documents, select the document you require.

Appendix B: 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) 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 links

Managed Element field descriptions on page 93
Applying configuration changes on page 91
Managed element worksheet for SAL Gateway on page 91

Index

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

P

R

S

T

U

V

W